#2

501.37212X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): M. KAYASHIMA, et al

Serial No.:

Filed: May 19, 1999

Title: NETWORK MANAGEMENT SYSTEM

Group:

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

May 19, 1999

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanee Patent Application No.(s) 10-136614 filed May 19, 1998.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/nac
Attachment
(703) 312-6600

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年 ５月１９日

出 願 番 号
Application Number: 平成１０年特許願第１３６６１４号

出 願 人
Applicant (s): 株式会社日立製作所

１９９９年 ４月 ９日

特 許 庁 長 官
Commissioner,
Patent Office 伊佐山建志

出証番号 出証特平１１－３０２１９６２

【書類名】　特許願

【整理番号】　PNT970452

【提出日】　平成10年 5月19日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/00
H04L 9/14
H04L 9/16
H04L 9/30
H04L 9/32
G06F 17/60

【発明の名称】　ファイアウォール統括管理システム

【請求項の数】　9

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　藤山　達也

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　萱島　信

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　寺田　真敏

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区戸塚町５０３０番地　株式会社日立製作所ソフトウェア開発本部内

【氏名】　荻野　孝明

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代表者】　金井　務

【代理人】

【識別番号】　100061893

【弁理士】

【氏名又は名称】　髙橋　明夫

【電話番号】　03-3661-0071

【選任した代理人】

【識別番号】　100086656

【弁理士】

【氏名又は名称】　田中　恭助

【電話番号】　03-3661-0071

【手数料の表示】

【予納台帳番号】　011626

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ファイアウォール統括管理システム

【特許請求の範囲】

【請求項１】　ネットワークの管理単位間にファイアウォールを設けたネットワークに適用するファイアウォール統括管理システムにおいて、

ファイアウォールに管理情報の設定をおこなうための管理サーバを設け、

その管理サーバのマネージャプログラムから、設定情報を送信することによって、

ネットワーク形態から見て、あるファイアウォールに隔てられて直接通信できないファイアウォールに対しても、管理情報の設定をおこなえることを特徴とするファイアウォール統括管理システム。

【請求項２】　各々のファイアウォールは、

中継プログラムと、

中継経路情報を格納する中継経路テーブルとを有し、

前記マネージャプログラムから、通信要求があったときには、

前記中継プログラムは、前記中継テーブルを参照し、適切な中継先のファイアウォールに通信要求を出し、

次の経路となるファイアウォールに接続を順次中継して、

最終的に、前記マネージャプログラムが、設定対象となるファイアウォールに対して設定情報を送信できるようにすることを特徴とする請求項１記載のファイアウォール統括管理システム。

【請求項３】　前記接続を中継するファイアウォールの中継プログラムが、前記管理サーバに対する認証をおこなうことを特徴とする請求項２記載のファイアウォール統括管理システム。

【請求項４】　前記管理サーバ上の前記マネージャプログラムが、前記接続を中継するファイアウォールに対する認証をおこなうことを特徴とする請求項２記載のファイアウォール統括管理システム。

【請求項５】　前記管理サーバ上の前記マネージャプログラムと、前記中継サーバの前記中継プログラムの通信を暗号化することを特徴とする請求項２ない

し請求項４記載のいずれかのファイアウォール統括管理システム。

【請求項６】　各々のファイアウォールに、エージェントプログラムを設け

そのファイアウォールに管理情報の設定をおこなうときには、

前記エージェントプログラムは、前記管理サーバ上のマネージャプログラムのエージェントとして、管理情報の設定を自らにおこなうことを特徴とする請求項１ないし請求項５記載のファイアウォール統括管理システム。

【請求項７】　前記ファイアウォールにあるエージェントプログラムは、

前記管理サーバのマネージャプログラムから、設定情報を送信されたときに、

前記管理サーバに対する認証をおこなうことを特徴とする請求項６記載のファイアウォール統括管理システム。

【請求項８】　前記管理サーバのマネージャプログラムは、

サービスを受けるクライアントのクライアントアドレスと、サービスを提供するサーバのサーバアドレスとから、設定情報を送信するファイアウォールを特定することを特徴とする請求項１ないし請求項７記載のいずれかのファイアウォール統括管理システム。

【請求項９】　前記管理サーバのマネージャプログラムは、

管理者から入力された情報にしたがって、

設定情報を生成し、各々のファイアウォールに設定情報を送信することを特徴とする請求項１ないし請求項８記載のいずれかのファイアウォール統括管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ファイアウォール統括管理システムに係り、大規模なネットワークでセキュリティのために複数のファイアウォールが必要なイントラネットなどに好適なシステムであって、それら複数のファイアウォールに対して、一括して管理のための情報を設定することを可能にすることにより、管理者の労力の軽減に資するファイアウォール統括管理システムに関する。

【０００２】

【従来の技術】

インターネットのようなオープンなネットワーク上で、あたかも専用線のような使い勝手を実現するＶＰＮ（Virtual Private Network）が注目を集めつつある。このＶＰＮ技術では、私的なネットワークをオープンなネットワーク上に接続するため、不正侵入を阻止するためのセキュリティ対策として、ファイアウォール（Firewall）を用いるのが一般的になっている。このファイアウォールでは、特定のユーザのみにアクセスを許可するアクセス制御や、データの暗号化によりシステムとしての安全度を高めている。

【０００３】

普通、ファイアウォールは、各ネットワークの管理単位（インターネットでは、「ドメイン」）間に設けられるので、複数のネットワークの管理単位を接続するときは、システム全体として複数のファイアウォールが存在することになる。そして、これらのファイアウォールの設定は、それぞれ独立に行うわけではなく、相互に関連を持つため、全体を統括して管理する必要がある。

【０００４】

このようなＶＰＮに関係する全てのファイアウォールの設定を、統括的に管理する製品として、CheckPoint社の「FireWall-1」がある。FireWall-1は、「管理モジュール」と「ファイアウォールモジュール」により構成されており、個々のファイアウォールに対する設定を、一つの管理モジュールからおこなうことができる。セキュリティに関する定義情報であるセキュリティポリシーを生成すると、管理モジュールは、対象となるファイアウォールモジュールに対して設定データを送付する。

【０００５】

【発明が解決しようとする課題】

FireWall-1に代表される従来技術は、管理モジュールが複数のファイアウォールモジュールを管理することにより、各ファイアウォールが保護するネットワークや利用ユーザの設定を管理モジュールから一括しておこなうことができる。

【０００６】

しかしながら、上記従来技術では、実際にファイアウォールに対して、管理情報を設定しなければならない管理者の労力軽減ということについては、限定的なものに止まっていた。というのも、特に認証されたユーザのみ複数のファイアウォールを越える通信を実行できるように設定するには、管理者は、以下のように二段階からなる煩わしい作業をおこなう必要があったからである。

【０００７】

・通信経路上にあるファイアウォールを特定する。

【０００８】

・特定した各ファイアウォールにユーザ登録と動作設定とをおこなう。

【０００９】

また、上記従来技術は、ファイアウォールモジュールにより保護された内部ネットワーク上に設置された内部ファイアウォールモジュールに設定情報を送信するなどの管理作業をするには、管理モジュールが直接内部ファイアウォールモジュールへ通信可能であることを必要とする。

【００１０】

しかしながら、以下の状況のような場合では、ファイアウォールモジュールとの通信が不可能になる。

【００１１】

・中継の経路上にあるファイアウォールモジュールが、管理用通信プロトコルをフィルタリングして通さないとき

・内部ネットワークがローカルアドレスを使用するとき

このような場合には、ローカルなネットワークの内部の端末から管理情報を設定しなければならなかったり、管理通信プロトコルをフィルタリングしないように設定するなど、いずれも管理者にとっては煩雑な作業が必要であった。

【００１２】

本発明は、上記従来技術の問題点を解決するためになされたもので、イントラネット、ＶＰＮのような複数のファイアウォールを有するネットワークシステムにおいて、それらのファイアウォールを統括的に管理して、ファイアウォールに

対する管理情報の設定を一括しておこなえるようにして、ネットワーク管理者の労力の軽減に資するファイアウォール統括管理システムを提供することを目的とする。

【００１３】

【課題を解決するための手段】

上記目的を達成するために、本発明のファイアウォール統括管理システムに係る発明の構成は、ネットワークの管理単位間にファイアウォールを設けたネットワークに適用するファイアウォール統括管理システムにおいて、ファイアウォールに管理情報の設定をおこなうための管理サーバを設け、その管理サーバのマネージャプログラムから、設定情報を送信することによって、ネットワーク形態から見て、あるファイアウォールに隔てられて直接通信できないファイアウォールに対しても、管理情報の設定をおこなえるようにしたものである。

【００１４】

より詳しくは、上記ファイアウォール統括管理システムにおいて、各々のファイアウォールは、中継プログラムと、中継経路情報を格納する中継経路テーブルとを有し、前記マネージャプログラムから、通信要求があったときには、前記中継プログラムは、前記中継テーブルを参照し、適切な中継先のファイアウォールに通信要求を出し、次の経路となるファイアウォールに接続を順次中継して、最終的に、前記マネージャプログラムが、設定対象となるファイアウォールに対して設定情報を送信できるようにするようにしたものである。

【００１５】

また詳しくは、上記ファイアウォール統括管理システムにおいて、前記接続を中継するファイアウォールの中継プログラムが、前記管理サーバに対する認証をおこなうようにしたものである。

【００１６】

別に詳しくは、上記ファイアウォール統括管理システムにおいて、前記管理サーバ上の前記マネージャプログラムが、前記接続を中継するファイアウォールに対する認証をおこなうようにしたものである。

【００１７】

さらに詳しくは、上記ファイアウォール統括管理システムにおいて、前記管理サーバ上の前記マネージャプログラムと、前記中継サーバの前記中継プログラムの通信を暗号化するようにしたものである。

【００１８】

さらにまた詳しくは、上記ファイアウォール統括管理システムにおいて、各々のファイアウォールに、エージェントプログラムを設け、そのファイアウォールに管理情報の設定をおこなうときには、前記エージェントプログラムは、前記管理サーバ上のマネージャプログラムのエージェントとして、管理情報の設定を自らにおこなうようにしたものである。

【００１９】

また詳しくは、上記ファイアウォール統括管理システムにおいて、前記ファイアウォールにあるエージェントプログラムは、前記管理サーバのマネージャプログラムから、設定情報を送信されたときに、前記管理サーバに対する認証をおこなうようにしたものである。

【００２０】

さらに詳しくは、上記ファイアウォール統括管理システムにおいて、前記管理サーバのマネージャプログラムは、サービスを受けるクライアントのクライアントアドレスと、サービスを提供するサーバのサーバアドレスとから、設定情報を送信するファイアウォールを特定するようにしたものである。

【００２１】

さらにまた詳しくは、上記ファイアウォール統括管理システムにおいて、前記管理サーバのマネージャプログラムは、管理者から入力された情報にしたがって、設定情報を生成し、各々のファイアウォールに設定情報を送信するようにしたものである。

【００２２】

【発明の実施の形態】

以下、本発明に係る一実施形態を、図１ないし図２３を用いて説明する。

【００２３】

〔ファイアウォール統括管理システムのネットワーク構成〕

先ず、図１を用いて本実施形態に係るファイアウォール統括管理システムのネットワーク構成について説明する。

図１は、本実施形態に係るファイアウォール統括管理システムのネットワーク構成図である。

【００２４】

本実施形態では、プロトコルとしてインターネットのデファクトスターンダードになっているＴＣＰ（Transmission Control Protocol）／ＩＰ（Internet Protocol）を用いるものとして説明する。

【００２５】

ドメイン１２ａ～１２ｅは、ネットワークが管理される単位であり、一つのドメインは、同じ方針で管理されている。また、各ドメインは、不特定多数のユーザがアクセス可能なオープンなネットワークであるインターネット１１で結ばれている。さらに、各ドメインと外部のネットワークとの間には、外部からの不正侵入を防ぐためのアクセス制御をおこなう装置であるファイアウォール１４ａ～１４ｄが設けられている。

【００２６】

ドメイン２には、管理サーバ１３と管理端末１５が接続されている。管理サーバ１３は、ファイアウォールを管理する機能を提供するサーバである。管理端末１５は、管理者がファイアウォールの管理作業をおこなうために設けられた端末である。従来では、ファイアウォールの管理は、ファイアウォールと同じドメインに接続されている端末からおこなっていたが、本発明では、これらの管理サーバ１３と管理端末１５により、他のドメインに接続されているファイアウォールの管理情報も設定できるところに特徴がある。

【００２７】

なお、本実施形態では、管理作業用のユーザインタフェースを提供する管理端末１５を用意したが、ネットワークの構成上、管理サーバから管理作業をおこなうようにしても良い。

【００２８】

各ドメイン１２ａ～１２ｄは、オープンなインターネットを利用して、仮想的にプライベートなネットワークとして利用する、いわゆるＶＰＮ（Virtual Private Network）を実現しているものとする。その際に、セキュリティのためには、ファイアウォールは必須の設備であるということができる。

【００２９】

〔ファイアウォール統括管理システムの各ハードウェア構成〕

次に、図２ないし図４を用いて本実施形態に係るファイアウォール統括管理システムを構成している各々のハードウェア構成について説明する。

先ず、図２を用いて本実施形態の管理サーバのハードウェア構成について説明する。

図２は、本実施形態に係る管理サーバ１３のハードウェア構成図である。

【００３０】

管理サーバ１３は、プロセッサ２１と、固定ディスク２２と、メモリ２７と、入出力制御部２１１と、ネットワーク制御部２１３とで構成される。

【００３１】

プロセッサ２１は、計算機内のハードウェア間の制御とプログラムの処理をおこなうユニットである。固定ディスク２２は、大容量の補助記憶装置であり、プログラムやテーブルを格納する装置である。メモリ２７は、プログラムをロードしたり、一時的なデータを格納する装置であり、通常は半導体素子で構成される。入出力制御部２１１は、外部に記憶された入出力装置、例えば、ディスプレイやキーボード２１２などを制御する。ネットワーク制御部２１３は、他の計算機との間の回線を制御する部分である。

【００３２】

固定ディスク２２には、本発明のファイアウォール統括管理システムを実現するためのプログラムと各種のテーブルが格納される。マネージャプログラム２３は、管理サーバ上で動作する管理プログラムであり、管理者から入力された情報に基づき、ファイアウォールに設定するための制御情報を生成し、ファイアウォールに送信する機能を持つ。認証・暗号通信モジュール２２ａは、マネージャプ

ログラム２３から呼び出され、認証、暗号通信をおこなう機能を受け持つ。ファイアウォール構成情報テーブル２４は、ファイアウォールとドメインとの接続関係を記載したテーブルである。ユーザ情報テーブル２５は、様々なユーザ情報を格納するテーブルであり、ユーザ毎のネットワーク利用形態情報と利用経路情報とから成っている。中継経路テーブル２６は、送信先アドレスと次の接続先アドレスである中継先アドレスとを記載したテーブルであり、設定情報をファイアウォールに送信するときに、接続を中継するファイアウォールのアドレスを格納する。

【００３３】

なお、ここに出てきたテーブルの内容と機能については後に詳細に説明する。

【００３４】

一方、メモリ２７は、上記のようにプログラムを固定ディスクからロードしてきて格納したり、一時的なデータを保持するための装置であり、論理的に各エリアに分割して用いられる。マネージャプログラムエリア２８は、マネージャプログラム２２を格納するエリア、認証・暗号通信モジュールエリア２９は、認証・暗号通信モジュールがロードされるエリア、ファイアウォール設定情報テーブルエリア２１５は、ファイアウォールの管理情報設定のときに、ダイナミックに生成されるファイアウォール設定情報テーブル２１５を格納するエリアであり、経由ファイアウォールテーブルエリア２１４は、経由ファイアウォールテーブルを格納するエリア、中継経路テーブルエリア２１０は、中継経路テーブルエリアを格納するエリアである。ファイアウォール設定情報テーブル２１５と経由ファイアウォールテーブルエリア２１４についても後述する。

【００３５】

次に、図３を用いて本実施形態のファイアウォールのハードウェア構成について説明する。

図３は、本実施形態に係るファイアウォール１４ａ～１４ｄのハードウェア構成図である。

【００３６】

ファイアウォール１４ａ～１４ｄは、プロセッサ３１と、固定ディスク３２と

、メモリ３６と、ネットワーク制御部３１３とで構成される。各々の機能は、管理サーバ１３のときと同様である。

【００３７】

ファイアウォール１４ａ～１４ｄの固定ディスク３２にも、管理サーバ１３のときと同様に、本発明のファイアウォール統括管理システムを実現するためのプログラムと各種のテーブルが格納される。エージェントプログラム３３は、ファイアウォール上でマネージャプログラムのエージェント（代理人）として働くプログラムであり、マネージャプログラムから送信されてくるファイアウォールの設定情報を受信し、それをファイアウォールが持っている各テーブルに設定する。中継経路テーブル３５は、管理サーバ１３のときと同様に、送信先アドレスと次の接続先アドレスである中継先アドレスとを記載したテーブルであり、設定情報をファイアウォールに送信するときに、接続を中継するファイアウォールのアドレスを格納する。中継プログラム３４は、ファイアウォールの設定情報を持つパケットを設定対象となるファイアウォールに送信するときに、その経路にあたるファイアウォールが、接続を中継するプログラムであり、前記中継経路テーブル３５に基づいて接続を次のファイアウォールに中継する機能を持つ。認証・暗号通信モジュール３３ａは、エージェントプログラム３３から呼び出され、認証、暗号通信をおこなう機能を受け持つ。ユーザ登録テーブル３１２は、ユーザ登録情報を格納し、ユーザがサービスを受けるときに認証をおこなうためのテーブルである。アクセス制御テーブル３１３は、ユーザがサービスを受けるときに必要とする各種情報を格納するテーブルである。経路制御テーブル３１４は、ユーザがサービスを受けるときのパケットの経路情報を格納するテーブルである。

【００３８】

また、ファイアウォール１４ａ～１４ｄのメモリ３６には、エージェントプログラムエリア３７と、中継プログラムエリア３８と、中継経路テーブルエリア３９と、認証・暗号通信モジュールエリア３１０に分割されてデータが格納される。エージェントプログラムエリア３７は、エージェントプログラム３３を格納するエリア、中継プログラムエリア３８は、中継プログラム３４が格納されるエリア、中継経路テーブルエリア３９は、中継経路テーブルを格納するエリア、認証

・暗号通信モジュールエリア３１０は、認証・暗号通信モジュールがロードされるエリアである。

【００３９】

次に、図４を用いて本実施形態の管理端末のハードウェア構成について説明する。

図４は、本実施形態に係る管理端末１５のハードウェア構成図である。

【００４０】

管理端末１５は、プロセッサ４１と、固定ディスク４２と、メモリ４５と、入出力制御部４６と、ネットワーク制御部４８とで構成される。管理端末１５も、各々の機能は、管理サーバ１３のときと同様である。

【００４１】

管理端末１５上の固定ディスク４２には、ユーザインターフェイスプログラム４３が、格納されていて、実行されるときには、メモリ上のユーザインターフェイスプログラムにロードされる。ユーザインターフェイスプログラムは、ネットワークの管理者にファイアウォールの制御操作のためのユーザインターフェイスを提供するプログラムである。

【００４２】

〔ファイアウォール統括管理システムのファイアウォール設定処理〕

次に、図５ないし図１９を用いて本発明に係るファイアウォール統括管理システムにおいて、ファイアウォールの設定をする処理について説明する。

図５は、本発明に係るファイアウォール統括管理システムが、ファイアウォールの設定をする処理を模式的に示した図である。

【００４３】

この図５で示された例では、図１に示したシステム構成のもとで、特に認証されたユーザ１９７のみがクライアントからサーバ１９９にアクセスできるようにファイアウォールに設定する場合を想定している。

【００４４】

管理サーバ１３が、このようなファイアウォールの設定処理をおこなうときには、以下の処理を順におこなうことになる。これを、図５をふまえて項を分けて

説明しよう。

【００４５】

（１）設定対象ファイアウォールを特定する処理１９１

（２）ファイアウォール毎に設定情報を生成する処理１９２

（３）ファイアウォール毎の設定情報を各ファイアウォールに送信する処理１９３

（４）各ファイアウォールが設定情報を受信し、それを設定する処理１９４

（５）ファイアウォールが接続を中継する処理１９５

（１）設定対象ファイアウォールを特定する処理１９１

先ず、図６ないし図１０を用いて設定対象ファイアウォールを特定する処理１９１について説明する。

図６は、管理者が、設定情報を入力するときの管理端末１５上の入力画面５１を示す図である。

図７は、管理サーバ１３上のファイアウォール構成情報テーブル２４を示す図である。

図８は、マネージャプログラム２２が設定するファイアウォールを特定する処理を示すフローチャートである。

図９は、経由ドメインリスト２１４の内容を状態毎に示した図である。

図１０は、管理サーバ１３上の経由ファイアウォールテーブル２１４を示す図である。

【００４６】

ファイアウォールとして、ネットワークの防衛のために有効に機能するためには、そのネットワークの形態から見て設定が必要なファイアウォールを特定し、そのファイアウォールに対して、サービスを受ける利用者の利用形態を想定した設定をする必要がある。そのために、先ず管理者は、図５に示される管理端末１５から、必要な設定情報を入力する。

【００４７】

ユーザ識別子（グローバルユーザ名）５２は、サービスを受けるネットワーク全域において、一意的でグローバルに通用する名称である。クライアントアドレ

ス５３は、ユーザが利用するクライアントのアドレスであり、サーバアドレス５４は、ユーザがサービスを受けるサーバのアドレスである。このアドレスは、計算機またはネットワークを一意的に識別するアドレスであり、表記の仕方については、ＤＮＳ（Domain Name System）に基づくドメイン形式で記述し、ネットワーク全体で通用するアドレスにしておく必要がある。

【００４８】

サービス名５５には、ユーザが利用するサービス名を入力する。この図５に示される例は、グローバルユーザ名が「ａｂｃ」であるユーザが、「ドメイン１」から「ドメイン３」に「ｔｅｌｎｅｔ」でアクセスするサービスを前提として、ファイアウォールの設定をおこなう場合である。

【００４９】

管理端末１５からの入力が終わると、管理端末１５上のユーザインタフェースプログラム４３は、入力画面５１に入力された情報を、管理サーバ１３に送信する。そして、管理サーバ１３上のマネージャプログラム２３は、送信されてくる入力情報を取得する。

【００５０】

設定するファイアウォールを特定するためには、管理サーバ１５のマネージャプログラム２３がネットワークの形態を押さえる必要がある。そのために、ドメインとファイアウォールの接続関係を記述したものが図７に示されるファイアウォール構成情報テーブル２４である。

【００５１】

ファイアウォール構成情報テーブル２４は、図７に示されるように、ドメインを示すドメイン名フィールド６１と、そのドメインに接続されているファイアウォールを示すファイアウォール名フィールド６２と、ドメイン名フィールド６１に記述したドメインとファイアウォールを隔てて隣接するドメインを示す隣接ドメイン名フィールド６３から構成されている。

【００５２】

本実施形態で採り上げる図１に示すネットワーク環境の場合、ドメイン２（１２ｂ）には、ファイアウォール１（１４ａ）とファイアウォール２（１４ｂ）が

接続されている。そして、ファイアウォール１（１４ａ）側には、ドメイン１（１２ａ）が隣接しており、ファイアウォール２（１４ｂ）側には、インターネット（１１）が隣接している。このときには、ファイアウォール構成情報テーブル２４の各フィールドには、エントリ６４ａ，６４ｂ，６４ｃ，６４ｆに示す内容が登録される。

【００５３】

次に、図８および図９を用いてマネージャプログラム２３が、設定対象ファイアウォールを特定する処理手順を説明する。

【００５４】

この処理は、マネージャプログラム２３が、ユーザの利用するクライアントアドレス５３、サーバアドレス５４、およびファイアウォール構成情報テーブル２４とを用いて、経由するファイアウォールを特定することにより、設定対象となるファイアウォールを決定するものである。

【００５５】

ドメイン形式のアドレスは、ホスト名とクライアントの属するドメイン名が合成された形式をとる。したがって、図７（ａ）に示されるように、マネージャプログラム２３は、まず、ドメイン形式で与えられたクライアントアドレス５３から、ホスト名を除くことによりクライアントの属するドメイン名（クライアントドメイン名）を取得する。例えば、ドメイン形式が、「www.xyz.co.jp」であるときには、wwwがホスト名であり、クライアントドメイン名は、xyz.co.jpとなる。そして、経由ドメインリスト２１４の先頭に得られたクライアントドメイン名を追加する（Ｓ７１）。

【００５６】

経由ドメインリスト２１４は、クライアントからサーバまでの間に経由するドメイン名を保存するリストである。経由ドメインリスト２１４が具体的にどの様に用いられるかについては、後に図９を用いて詳細に説明する。

【００５７】

次に、クライアントドメイン名に対して、処理Ａ（Ｓ７４）を実行する（Ｓ７２）。処理Ａは、再帰的呼出し手続きであり、経由ドメインリストを取得する処

理である。したがって、この処理を抜け出てきたときには、クライアントからサーバまでの経由ドメインリストが完成されている。

【００５８】

最後に、経由ドメインリスト中の連続するドメイン名とファイアウォール構成情報テーブルとから、その間のファイアウォール名を取得することにより、経由するファイアウォールのリスト（経由ファイアウォールリスト）を取得する（Ｓ７３）。この経由ファイアウォールリストは、図１０に示される経由ファイアウォールテーブル２１４のエントリとして格納される。

【００５９】

経由ファイアウォールテーブル２１４は、設定対象ファイアウォールを特定する処理の結果を格納するためのテーブルであり、クライアントアドレスフィールド８１とサーバアドレスフィールド８２と経由ファイアウォールリストフィールド８３とから構成される。クライアントアドレスフィールド８１とサーバアドレスフィールド８２は、それぞれクライアントのアドレスとサーバのアドレスを格納するフィールドである。経由ファイアウォールリストフィールド８３は、前述の如く、設定対象ファイアウォールを特定する処理の結果として、クライアントアドレス５３からサーバアドレス５４までの経路上にあるファイアウォールのリストを格納したものある。すなわち、この経由ファイアウォールリストフィールド８３に記載された一連のファイアウォールが、クライアントがサーバからサービスにあたって、マネージャプログラム２３が、設定対象とするファイアウォールである。

【００６０】

次に、上記の処理Ａ（Ｓ７４）について説明する。

【００６１】

この処理Ａに与えられる引数は、ドメイン名、ファイアウォール構成情報テーブル２４、経由ドメインリスト２４１である。また、この処理Ａは、再帰的呼出し手続き（Ｒｅｃｕｒｃｉｖｅ　Ｃａｌｌ）であることに注意する。

【００６２】

先ず、マネージャプログラム５３は、与えられたドメイン名とファイアウォー

ル構成情報テーブル２４のドメイン名フィールド６１とが一致するエントリを検索する。そして、一致したエントリの隣接ドメイン名フィールド６３に記載されたドメイン名からリストを作成する（Ｓ７５）。これを、隣接ドメイン名リストと言うことにする。

【００６３】

この隣接ドメイン名リストに要素がない場合（Ｓ７６）、処理Ａから抜ける。

【００６４】

隣接ドメイン名リストに要素がある場合（Ｓ７６）、そのリストからドメイン名を１つ選択する。選択したドメイン名が、経由ドメインリストで既に使用されているならば、隣接ドメイン名リストから別のドメイン名を選択する（Ｓ７７）。経由ドメイン名リストで使用されていなければ、経由ドメイン名リストに追加する（Ｓ７８）。

【００６５】

そして、今追加したドメイン名がサーバが属するドメイン名（サーバドメイン名）に等しいか否かを調べる（Ｓ７９）。追加したドメイン名がサーバが属するドメイン名（サーバドメイン名）に等しいならば（Ｓ７９）、経由ドメインリストを別領域に保存する（Ｓ７１０）。

【００６６】

この時点で保存されたドメインリストが、この処理の答えとなる経由ドメインリストになる。

【００６７】

そして、経由ドメインリストの一番最後に追加されたドメイン名を削除する。これは、手続きが再帰的呼出しを使っているため、経由ドメインの探索を元に戻して処理するために必要なる手続きである。

【００６８】

そして、隣接ドメインリストを調べる処理に戻る（Ｓ７６）。

【００６９】

追加したドメイン名がサーバドメイン名に等しくないならば（Ｓ７９）、追加したドメイン名を引数にして、再帰的に、処理Ａを呼び出す（Ｓ７１２）。

【００７０】

処理Ａから抜け出たときには、経由ドメインリストの一番最後に追加されたドメイン名を削除する（Ｓ７１３）。これも、処理Ａが、再帰的呼出しであるために、処理から抜けたときには、一番最後に追加されたドメイン名での探索は終了していることから必要になる処理である。

【００７１】

この処理Ａでは、再帰的な呼び出しを使っているために、クライアントからサーバへの道筋が複数ある場合にも、探索をすべての経路についておこなって、経由する可能性のある道筋をすべて見つけ出すことができることに注意しよう。

【００７２】

ここで、図９を用いて「ドメイン１」に属するクライアントから「ドメイン３」に属するサーバにアクセスする場合に、設定するファイアウォールを特定する処理を具体的に説明しよう。まず、「ドメイン１」を経由ドメインリストの先頭に追加する（Ｓ７１、図９（ａ））。次に、「ドメイン１」を処理Ａに渡す引数として、経由ドメインリストを取得する処理Ａ（Ｓ７４）を開始する（Ｓ７２）。まず、「ドメイン１」とドメイン名フィールド６１が一致するエントリとして６５ａを検出し、その隣接ドメイン名フィールド６３に記載された「ドメイン２」を隣接ドメインリストに加える（Ｓ７５）。次に、隣接ドメインリストから「ドメイン２」を選択する（Ｓ７６）。「ドメイン２」は経由ドメインリストにないので（Ｓ７７）、「ドメイン２」を経由ドメインリストに追加する（Ｓ７８、図９（ｂ））。「ドメイン２」は、サーバドメイン名「ドメイン３」に等しくないので（Ｓ７９）、「ドメイン２」を引数として、経由ドメインリストを取得する処理Ａ（Ｓ７４）を開始する（Ｓ７１２）。次に、「ドメイン２」を引数として、処理Ａ（Ｓ７４）を呼び出して、エントリ６４ｂとエントリ６４ｃから、隣接ドメインリストとして、「ドメイン２」と「ドメイン１」が得られる。「ドメイン１」の方は、既に経由ドメインリストに含まれているので、候補から省かれる（Ｓ７７）。したがって、この段階で図９（ｃ）に示される経由ドメインリストが得られる。

【００７３】

次に、ドメイン名「インターネット」を引数として、処理Ａ（Ｓ７４）が呼び出される。

【００７４】

「インターネット」をキーとして、得られる隣接ドメインは、エントリ６４ｆ，６４ｇ，６４ｈから、それぞれ、「ドメイン２」、「ドメイン３」、「ドメイン４」である。

【００７５】

「ドメイン２」は、やはり経由ドメインリストに既に存在しているので候補から省かれ、「ドメイン３」を経由ドメインリストに追加したときに、サーバドメイン名に等しくなるため（Ｓ７９）、これを答えとして保存する（Ｓ７１０）。このあと、追加したドメインである「ドメイン３」を削除する（Ｓ７１１）。そして、図９（３）の状態に戻り探索を続けることになる。

【００７６】

最終的に、図９（ｄ）の状態のときの経由ドメインリストが、この処理の答えであって、「ドメイン１」、「ドメイン２」、「インターネット」、「ドメイン３」が取得できる。

【００７７】

（２）ファイアウォール毎に設定情報を生成する処理１９２

次に、図１１ないし図１３を用いて管理サーバ１３上のマネージャプログラム２２が、各ファイアウォールに対して設定する情報を生成する処理について説明する。

図１１は、管理サーバ１３上のユーザ情報テーブル２５を示す図である。

図１２は、管理サーバ１３上のファイアウォール設定情報テーブル２１５を示す図である。

図１３は、登録ＩＤを生成する処理を示すフローチャートである。

【００７８】

（１）の処理により、設定対象のファイアウォールを特定した後、管理サーバ１３上のマネージャプログラム２２は、各ファイアウォールに対して設定する情報

を生成する。

【００７９】

最終的に、必要な情報が生成されると、図１１に示されるユーザ情報テーブル２５と図１２に示されるファイアウォール設定情報テーブル２１５に格納されることになる。ここで、ユーザ情報テーブル２５は、ユーザ識別子（グローバルユーザ名）毎に、サービスを受けるときの利用形態と利用経路情報としてまとめたテーブルである。また、ファイアウォール設定情報テーブル２１５は、管理サーバのメモリ情報にダイナミックに作られるテーブルであり、後に説明するファイアウォールへ情報を設定するときのリクエストパケットを生成するときに用いられるテーブルである。

【００８０】

（ａ）登録ＩＤの生成

先ず、マネージャプログラム２８は、登録ＩＤを生成する。登録ＩＤとは、各ファイアウォールがサービスを受けるユーザに対して、認証をおこなうために用いる識別子である。これは、ユーザ毎、ファイアウォール毎に一意的な名称を用いる必要がある。

【００８１】

これを図１２に示したユーザ情報テーブル２５のエントリ１２６ｃを例にとって説明しよう。

【００８２】

（１）と（２）の処理が終わった段階で、グローバルユーザ名１２１「ａｂｃ」、クライアントアドレス１２２「ドメイン１」、サーバアドレス１２３「ドメイン３」、サービス／プロトコル１２４「ｔｅｌｎｅｔ／ＴＣＰ」の値は設定されている。

【００８３】

利用経路情報リストフィールド１２５には、［ファイアウォール名　登録ＩＤ］がペアとなって、リスト構造で格納される。このエントリ１２６ｃには、［ファイアウォール１　ＡＢＣ］、［ファイアウォール２　ＡＢｃ］、［ファイアウォール３　Ａｂｃ］が格納されていることが示されている。これまで述べてきた

処理で設定対象となるファイアウォールは、ファイアウォール１、ファイアウォール２、ファイアウォール３であることは、求まっているので各々のファイアウォール毎に登録ＩＤを生成する処理をおこなうわけである。

【００８４】

次に、図１３のフローチャートの順を追いながら、マネージャプログラム２３が登録ＩＤを生成する処理について説明する。

【００８５】

マネージャプログラム２３は、図１１のユーザ情報テーブル２５を検索することにより、入力画面５１から取得したグローバルユーザ名５２が、設定対象ファイアウォールに登録されているかをチェックする（Ｓ１３１）。登録ＩＤは、グローバルユーザ名と、ファイアウォールが同じときには、同じになるものと約束するからである。

【００８６】

ユーザ情報テーブルを検索して、登録されているときには（Ｓ１３２）、ステップ１３７に進む。

【００８７】

登録されていないときには（Ｓ１３２）、登録ＩＤ候補を生成する（Ｓ１３３）。ここで、登録ＩＤ候補の生成処理は、第一候補をグローバルユーザ名をそのまま用いることにし、第二候補以降については、グローバルユーザ名の後ろに数字をつけたり（ａｂｃ１，ａｂｃ２，…）、大文字と小文字を変える（ＡＢＣ，ＡＢｃ，…）などの方法により実現できる。

【００８８】

さて、登録ＩＤは、各ファイアウォールで、サービスを受けるときに認証に使われるものである。したがって、同じファイアウォールで既にその登録ＩＤ候補が衝突することがないかを確認する必要がある。そのため、生成した登録ＩＤ候補を、ファイアウォール上のエージェントプログラム３３に送信する（Ｓ１３４）。マネージャプログラムとエージェントプログラムとの間の登録ＩＤ候補の送受信は、Ｔｅｌｎｅｔ等のアプリケーションと同様に、プロトコルとして、ＴＣＰ／ＩＰを用いることにして、両者の間でコネクションを確立し、そのコネクシ

ョン上でパケットを送受信することにより実現できる。

【００８９】

ファイアウォール上のエージェントプログラム３３は、送られてきた登録ＩＤ候補が、そのファイアウォール上で既に使われているか否かを確認し、その結果を管理サーバ上のマネージャプログラム２２に送信する（Ｓ１３５）。その結果、その登録ＩＤ候補が設定対象ファイアウォール上で既に使われていることがわかれば（Ｓ１３６）、別の登録ＩＤ候補を生成する（Ｓ１３２）。

【００９０】

まだ使用されていない場合には（Ｓ１３６）、それを登録ＩＤとする。

【００９１】

一つの設定対象の処理が終わると、次の設定対象ファイアウォールを取り出し、すべての設定対象ファイアウォールについて、同様にステップ１３１からステップ１３６の処理を繰り返す（Ｓ１３７）。

【００９２】

そして、全ての設定対象ファイアウォールについて登録ＩＤが確定したとき（Ｓ１３７）、ユーザ情報テーブル２５にエントリを追加する（Ｓ１３８）。

【００９３】

ここで、具体例を採って説明しよう。図１１に示すユーザ情報テーブル１２１に、エントリ１２６ａとエントリ１２６ｂだけが登録されているとし、図５に示す入力がおこなわれたとする。

【００９４】

（１）の設定対象ファイアウォールを特定する処理により、設定をおこなうファイアウォールは、「ファイアウォール１」、「ファイアウォール２」、「ファイアウォール３」であることがわかっている。エントリ１２６ａには、グローバルユーザ名が「ａｂｃ」のユーザがファイアウォール１に登録ＩＤ「ＡＢＣ」として登録されていることが分かるのでなにもしない（Ｓ１３１，Ｓ１３２）。

【００９５】

ファイアウォール２とファイアウォール３については、該当する登録ＩＤがないので、新規に登録ＩＤを生成する。

【００９６】

管理サーバ１３上でファイアウォール２とファイアウォール３に登録する登録ＩＤ候補を、それぞれ「ＡＢｃ」、「Ａｂｃ」と生成したとする（Ｓ１３３）。

【００９７】

マネージャプログラム３２は、ファイアウォール上のエージェントプログラム３３へそれらが使われていないと問い合わせおこない、それらが各々のファイアウォール上で使われていないという結果を得たとする（Ｓ１３４，Ｓ１３５，Ｓ１３６）。

【００９８】

その結果により、登録ＩＤとして、ファイアウォール２には「ＡＢｃ」、ファイアウォール３には「Ａｂｃ」を用いることが確定し、ユーザ情報テーブル２５にはエントリ１２６ｃが図１１の如く追加される。

【００９９】

（ｂ）ファイアウォール設定情報テーブル２１５の設定

これまで得られてきた情報を基にして、マネージャプログラム２３は、最終的に、図１２に示されるファイアウォール設定情報テーブル２１５に値を設定する。次の各設定対象ファイアウォールに対して設定情報を送信する処理の段階では、このテーブルを基にして、各設定対象ファイアウォールに対して送信する情報を生成するのである。

【０１００】

ファイアウォール設定情報テーブル２１５は、図１２に示される様に、設定対象ファイアウォール１４１、登録ＩＤ１４２、クライアントアドレス１４３、サーバアドレス１４４、サービス／プロトコル１４５、送信元アドレス１４６、送信先アドレス１４７から構成される。

【０１０１】

設定対象ファイアウォール１４１は、このテーブルのキーとなるフィールドであり、その名の如くその登録ＩＤに関して設定対象となるファイアウォールのアドレスが格納される。

【０１０２】

登録ＩＤ１４２は、（ａ）で説明してきた登録ＩＤが格納されるフィールドであり、クライアントアドレス１４３、サーバアドレス１４４、サービス／プロトコル１４５については、図１１に示したユーザ情報テーブル２５のときと同様である。

【０１０３】

送信元アドレス１４６は、このファイアウォールに対して、ユーザがサービスを受ける際に、パケットが直接送られてくる送信元のアドレスを示すフィールドである。逆に、送信先アドレス１４７には、ユーザがサービスを受ける際に、このファイアウォールが、パケットを直接送信する送信先のアドレスを示すフィールドである。これは、図１１に示される様に、サーバやクライアントに直接接しているときには、サーバアドレスやクライアントアドレスがそのまま格納され、ファイアウォールを経由するときには、ファイアウォールのアドレスが格納される。

【０１０４】

この送信元アドレス１４６と送信先アドレス１４７は、ユーザ情報テーブル２５のクライアントアドレス１２２、サーバアドレス１２３、および利用経路情報リスト１２５を基にして生成することができる。

【０１０５】

ここで具体例に基づいて説明しよう。

【０１０６】

図１２のエントリ１４８ｂに示されている設定対象ファイアウォールが、「ファイアウォール２」であるときには、図１１のユーザ情報設定テーブル２５のエントリ１２６ｃに基づいて、登録ＩＤ１４２に「ＡＢｃ」が、クライアントアドレス１４３に「ドメイン１」が、サーバアドレス１４４に「ドメイン３」が、サービス／プロトコル１４５に「ｔｅｌｎｅｔ／ＴＣＰ」が、それぞれ格納される。

【０１０７】

また、送信元アドレス１４６と送信先アドレス１４７には、利用経路情報リス

ト１２５の「ファイアウォール２」が格納されている前後のフィールドから、「ファイアウォール１」と「ファイアウォール３」が得られる。

【０１０８】

（３）ファイアウォール毎の設定情報を各ファイアウォールに送信する処理１９３

次に、図１４および図１５を用いてマネージャプログラム２３がファイアウォール毎の設定情報を各ファイアウォールに送信する処理１９３について説明する。

図１４は、マネージャプログラム２３が各ファイアウォールに送信するリクエストパケット１５１と、エージェントプログラム３３が管理サーバ１３に送信するリプライパケット１５１１のフォーマットを示す図である。

図１５は、管理サーバ１３上のマネージャプログラム２３と、ファイアウォール上のエージェントプログラム３３の通信プロトコルを示す図である。

【０１０９】

リクエストパケット１５１は、マネージャプログラム２３が各設定対象となるファイアウォールに対して情報を設定するときに使われるパケットである。リクエストパケット１５１は、図１４（ａ）に示される様に、コマンド１５２、作業対象１５３、登録ＩＤ１５４、クライアントアドレス１５５、サーバアドレス１５６、サービス／プロトコル１５７、送信元アドレス１５８、送信先アドレス１５９から構成される。このフォーマットは、必要なすべてのフィールドを挙げたものである。実際には、リクエストパケット１５１は、コマンド１５２、作業対象１５３毎に設定されるフィールドは異なっており、必要でないフィールドには、ＮＵＬＬ値が設定されることになる。

【０１１０】

リプライパケット１５１１は、エージェントプログラム３３がリクエストパケット１５１を受信したときに、ファイアウォール側で成否を示すために使われるパケットである。リクエストパケット１５１は、図１４（ｂ）に示される様に、リプライコード１５１２、コマンド１５１３、作業対象１５１４から構成される。

【０１１１】

さて、以下では図１４に示した具体例に基づき説明しよう。

【０１１２】

ここで、設定対象と想定しているファイアウォールは、ファイアウォール２である。

【０１１３】

パケット１５１０ａは、コマンド１５２が「ＡＤＤ」、作業対象が「ＵＳＥＲ」とされるパケットである。これは、登録ＩＤ１５４のフィールドが「ＡＢｃ」になっており、登録ＩＤ候補をファイアウォール２に登録するためのパケットである。

【０１１４】

パケット１５１０ｂは、コマンド１５２が「ＡＤＤ」、作業対象が「ＡＣＣＥＳＳ」とされるパケットである。このパケットが、リクエストパケット１５１の中で一番内容が多彩であり、送られてきた情報は、すべてファイアウォールのアクセス制御テーブル（後述）に格納される。各々のフィールドの意義はこれまで述べてきたとおりである。

【０１１５】

パケット１５１０ｃは、コマンド１５２が「ＡＤＤ」、作業対象が「ＲＯＵＴＥ」とされるパケットである。このパケットは、ユーザがサービスを受けるときのルーティング情報を設定するためのパケットである。サーバアドレス１５６のフィールドには、ユーザにサービスを提供するサーバのアドレス、送信元アドレス１５９には、サーバのアドレスに該当するパケットを受けたときに、中継先となるファイアウォールのアドレスが格納される。この例のパケットでは、ファイアウォール２が、「ドメイン３」にあるサーバのサービスを受けるパケットを受信したときには、中継先として、「ファイアウォール３」にパケットを送信することを指示するようになっている。送られてきた情報は、ファイアウォールの経路制御テーブル（後述）に格納される。

【０１１６】

マネージャプログラム２３は、これらのパケットを設定対象であるファイアウ

ォール２に送信する。

【０１１７】

ファイアウォール２のエージェントプログラム３３では、設定が正常に終了したときには、リプライコード１５１２に「０」を設定して、リプライパケット１５１１を管理サーバ１３のマネージャプログラム２３に送り返す。設定が正常に終了できなかったときには、リプライコード１５１２に「１」を設定して、リプライパケット１５１１を管理サーバ１３のマネージャプログラム２３に送り返す。ここで、リクエストパケット１５１のパケット１５１０ａ，１５１０ｂ，１５１０ｃに、それぞれ対応するリプライパケット１５１１が、パケット１５１５ａ，１５１５ｂ，１５１５ｃである。

【０１１８】

マネージャプログラム２３が、リプライコード１５１２が「１」のリプライパケット１５１１を受け取ったときには、再送信やエラー処理などのしかるべき処理をとることになる。

【０１１９】

次に、図１５を用いて、管理サーバ１３上のマネージャプログラム２３と、ファイアウォール上のエージェントプログラム３３が、リクエストパケット１５１とリプライパケット１５１１をやり取りするときの通信手順について説明しよう。

【０１２０】

マネージャプログラム２３は、（１）で設定対象とされたファイアウォールにつき、そのファイアウォール上のエージェントプログラム３３に対して、接続要求をおこなう（ＳＱ１６１）。

【０１２１】

マネージャプログラム２３とエージェントプログラム３３の間で相互認証を行う（ＳＱ１６２）。相互認証は、セキュリティを保つ上で必須の処理である。相互認証ＳＱ１６２に成功すると、両者で暗号鍵を取得する処理をおこなう（ＳＱ１６３）。暗号鍵が必要となるのは、両者がセキュリテイを保持するために暗号通信をおこなうことを前提としているからである。

【０１２２】

一方、相互認証ＳＱ１６２に失敗した場合には、そこで、そのファイアウォールに対する処理を打ち切り、他の設定対象ファイアウォール上のエージェントプログラムに対する通信処理に移る。

【０１２３】

暗号鍵取得処理ＳＱ１６３が終わると、エージェントプログラム３３が、通信が可能であることを通知する接続確認パケットをマネージャプログラム２３に送信する（ＳＱ１６４）。

【０１２４】

マネージャプログラム２３は、接続確認パケットを受信して接続を確認した後で、エージェントプログラム３３にリクエストパケット１５１を送信する（ＳＱ１６５）。リクエストパケット１５１は、暗号化されて送られることに注意しよう。

【０１２５】

エージェントプログラム３３は、暗号鍵を用いリクエストパケット１５１を復号して、その情報に基づき内部のテーブルに必要な値を設定する（ＳＱ１６６）。そして、その成否をリプライパケット１５１１で、をマネージャプログラム２３に通知する（ＳＱ１６７）。

【０１２６】

マネージャプログラム２３は、上記のシーケンスＳＱ１６１～シーケンスＳＱ１６７をすべての設定対象ファイアウォールに対して繰り返しおこなうことにより、複数のファイアウォールに対して、一括して必要な設定処理を実現することができる。

【０１２７】

なお、相互認証処理１６２は、ＩＳＯ／ＩＥＣ９７９８やＸ．５０９の認証方法に基づいて実装することにより、実現可能である。

【０１２８】

また、暗号鍵取得処理１６３については、例えば、マネージャプログラム２３とエージェントプログラム３３で生成したランダムデータを相互に交換し、両者

で共有した２つのランダムデータから同じ暗号鍵データを生成することにより、共有鍵方式の暗号通信をおこなうことが可能である。

【０１２９】

（４）各ファイアウォールが設定情報を受信し、それを設定する処理１９４

次に、図１６ないし図１８を用いて各ファイアウォールが設定情報を受信し、それを設定する処理１９４について説明する。

図１６は、ファイアウォール２上のユーザ登録テーブル３１２を示す図である。

図１７は、ファイアウォール２上のアクセス制御テーブル３１３を示す図である。

図１８は、ファイアウォール２上の経路制御テーブル３１４を示す図である。

【０１３０】

図で示されている値は、すべてファイアウォール２を例に採ったものである。

【０１３１】

ユーザ登録テーブル３１２は、登録ＩＤに対し、その登録ＩＤに合致する通信サービスのパケットを通過させるか否かを判断するときの認証情報を保持するテーブルであり、登録ＩＤ９１と、認証情報９２から構成されている。この認証情報９２は、ユーザに予め知らされていて、ユーザがサービスを受けるときに、そのクライアントから送信されてくる。ファイアウォールでは、その登録ＩＤに合致する認証情報が等しい否かにより、ユーザの認証をおこなう。

【０１３２】

ファイアウォール２は、図１４（ａ）に示された作業対象１５３が「ＵＳＥＲ」であるパケット１５１０ａを受けたときに登録ＩＤを設定し、それに対する認証情報を生成する。

【０１３３】

アクセス制御テーブル３１３は、ファイアウォール上の設定情報を持つテーブルとして、中心となるテーブルである。ファイアウォール２は、図１４（ａ）に示された作業対象１５３が「ＡＣＣＥＳＳ」であるパケット１５１０ｂを受けたときに、図１７に示される如く、それぞれ対応するフィールドにエントリ１０７

ａのように値を設定する。

【０１３４】

経路制御テーブル３１４は、ユーザがサービスを受けるときのパケットをルーティングするためのルーティングテーブルであり、送信先アドレス１１１と中継先アドレス１１２で構成されている。

【０１３５】

送信先アドレス１１１は、サービスを享受するためのサーバが属するドメインのアドレスである。また、中継先アドレス１１２は、送信先アドレス１１１に書かれたサーバのアドレスと一致するパケットが来たときに、それを中継するファイアウォールのアドレスである。

【０１３６】

この例では、ファイアウォール２が、ドメイン３に属するサーバにパケットを送るときには、中継先のファイアウォールは、ファイアウォール３になることを示している。すなわち、ファイアウォール２は、図１４（ａ）に示された作業対象１５３が「ＲＯＵＴＥ」であるパケット１５１０ｃを受けたときに、図１８に示される如く、エントリ１１３のように値を設定する。

【０１３７】

（５）ファイアウォールが接続を中継する処理１９５

次に、図１９および図２０を用いてファイアウォールが他のファイアウォールに対する接続を中継する処理について説明する。

図１９は、管理サーバ上とファイアウォール上の両者に置かれる中継経路テーブル１７１を示す図である。

図２０は、管理サーバ１３上のマネージャプログラム２３と、ファイアウォール上の中継プログラム３４、およびエージェントプログラム３３の三者の通信プロトコルを示す図である。

【０１３８】

中継テーブル１７１は、他のファイアウォールに接続を中継するために用いられるテーブルである。これは、予め管理者がネットワーク形態を調べ、設定しておく必要がある。また、この中継経路テーブル１７１は、他のファイアウォール

に接続するために、ファイアウォールと管理サーバとの両者に置かれることに注意しておこう。

【０１３９】

この図の値は、管理サーバ１３に置かれる中継経路テーブル１７１を想定している。すなわち、管理サーバ１３上のマネージャプログラム２３は、ファイアウォール３に設定するためのリクエストパケット１５１を送るときには、先ず、ファイアウォール２に対して接続要求をする。

【０１４０】

図には示さなかったが、ファイアウォール２上にある中継経路テーブル１７１には、送信先アドレス１７２が、「ファイアウォール３」で、中継先アドレス１７３も、「ファイアウォール３」のエントリがある。ファイアウォール２の中継プログラム３４は、ファイアウォール３が設定対象のファイアウォールであったときには、自らの持つ中継テーブル１７１の中継先アドレス１７３を見て、ファイアウォール３に接続要求にいく。その後、相互認証と暗号鍵の取得などの処理をおこなった後に、管理サーバ１３上のマネージャプログラム２３は、リクエストパケット１５１を送信する。

【０１４１】

次に、この通信手順を図２０を用いて説明しよう。

【０１４２】

マネージャプログラム２３は、中継経路テーブル１７１のエントリ１７４ａから、次の接続先をファイアウォール２（１４ｂ）に決定する（ＳＱ１８１）。

【０１４３】

そして、ファイアウォール２（１４ｂ）の中継プログラム３４に接続を要求する（ＳＱ１８２）。

【０１４４】

接続要求後、マネージャプログラムと中継プログラムとが相互認証処理ＳＱ１８３および暗号鍵取得処理ＳＱ１８４をおこなう。

【０１４５】

相互認証および暗号鍵取得に成功した場合には、中継プログラム３４は、ファ

イアウォール２（１４ｂ）上の中継経路テーブル１７１に基づいて、ファイアウォール３（１４ｃ）を中継先のファイアウォールであることを求める。その結果に基づいて、ファイアウォール２上の中継プログラム３４は、ファイアウォール３に接続することを決定し（ＳＱ１８５）、マネージャプログラム２３にファイアウォール３（１４ｃ）に接続することを通知する（ＳＱ１８６）。

【０１４６】

かつ、ファイアウォール２上の中継プログラム３４は、ファイアウォール３（１４ｃ）上のエージェントプログラム３３に接続要求をおこなう（ＳＱ１８７）。そして、その後は、図１５のシーケンスＳＱ１６１～シーケンスＳＱ１６７に従い、マネージャプログラム２３とエージェントプログラム３３との間で、相互認証処理ＳＱ１８８、暗号鍵取得処理ＳＱ１８９、接続確認ＳＱ１８１０がおこなわれ、管理サーバ上のマネージャプログラム２３と、ファイアウォール３上のエージェントプログラム３３上で通信が開始されることになる（ＳＱ１８１１）。

【０１４７】

すなわち、以上の手順により、マネージャプログラム２３とエージェントプログラム３３の間で、相互認証がおこなわれ、暗号で通信することが可能な安全なコネクションが確立することになる。

【０１４８】

なお、マネージャプログラム２３と中継プログラム３４との間の相互認証および暗号鍵取得の方法は、マネージャプログラム２３とエージェントプログラム３３との間の相互認証および暗号鍵取得の例と同じ方法が利用できる。

【０１４９】

〔ユーザがサービスを受けるときのファイアウォールの動作〕

次に、実際に、ユーザがクライアントからサーバに対して、サービスを受けるときにファイアウォールがどのように動作するかについて説明する。

【０１５０】

例として、図２１および図２３を用いて、図６に示した様にクライアントアドレスが「ドメイン１」で、サーバアドレスが「ドメイン３」で、サービス／プロ

トコルが「ＴＣＰ／ＩＰ」であるときのファイアウォールの処理について説明しよう。

図２１は、ファイアウォール１上のユーザ登録テーブル３１２を示す図である。

図２２は、ファイアウォール１上のアクセス制御テーブル３１３を示す図である。

【０１５１】

図２３は、ファイアウォール１上の経路制御テーブル３１４を示す図である。

【０１５２】

図１に示されたネットワークでは、ドメイン１（１２ａ）からパケットが送信されるので、先ず、ファイアウォール１（１４ａ）のチェックを受けることになる。

【０１５３】

ファイアウォール１（１４ａ）では、アクセスがあった場合に、図２２に示されたアクセス制御テーブル３１３を検索し、どの登録ＩＤに該当するを検索する。該当しない場合には、「サービスを受けるための登録ができていない」旨のメッセージを出し、ユーザのそれ以降のアクセスを拒否する。チェックに使う項目は、セキュリティの方針にしたがって、アクセス制御テーブルのすべての項目でチェックしても良いし、その一部の項目でチェックしても良い。

【０１５４】

この場合は、エントリ２０７ａの登録ＩＤ１０１の「ＡＢＣ」がこれに該当する。

【０１５５】

したがって、次に、図２１に示されるユーザ登録テーブル３１２により、ユーザ認証をおこなう。クライアントの方から認証情報が送られてくるので、ファイアウォール１（１４ａ）は、ユーザ登録テーブル３１２のエントリ２９３ａの認証情報と、合致するか否かを確認する。

【０１５６】

認証情報は、アクセスするときに、ユーザがパスワードを入力するイメージで

ファイアウォール側にその認証情報を送信するか、システムが自動的にその認証情報を送信するようにすれば良い。

【０１５７】

認証情報が間違っているときには、「ユーザの認証が失敗した」旨のメッセージを出し、サービスは、拒絶されることになる。

【０１５８】

認証情報が正しく送られてきたことを確認されたときには、ファイアウォール１（１４ａ）は、図２３に示された経路制御テーブルを参照して、次のファイアウォール２（１４ｂ）にパケットを中継する。この場合のパケットの送信先アドレスは、ドメイン３なのでエントリ２１３ａの中継先アドレスの値「ファイアウォール２」より次のファイアウォールが求められことになる。

【０１５９】

そして、パケットが中継されると、次のファイアウォール２（１４ｂ）でもおなじ処理がおこなわれる。

【０１６０】

ファイアウォール２（１４ｂ）では、図１６に示されるユーザ登録テーブル３１２と、図１７に示されるアクセス制御テーブル３１３とにより、アクセスの許可をする。用いられる登録ＩＤは、「ＡＢｃ」である。また、次の中継先を求めるのは、図１８に示される経路制御テーブルであり、このエントリ１１３ａにより、次の中継先がファイアウォール３であることを求める。

【０１６１】

このようにして、ファイアウォール１（１４ａ）、ファイアウォール２（１４ｂ）、ファイアウォール３（１４ｃ）のすべてにアクセスが許可されたときに、初めて、ドメイン１にいるクライアントは、ドメイン３のサーバからｔｅｌｎｅｔのサービスを享受できる。不正なアクセス、認証を受けていないユーザは、接続を拒否され、システムに侵入することができない。すなわち、各ファイアウォールでは、かくして不正なアクセスからシステムを防御する防火壁の役割を果たすことができる。

【０１６２】

【発明の効果】

本発明によれば、イントラネット、ＶＰＮのような複数のファイアウォールを有するネットワークシステムにおいて、それらのファイアウォールを統括的に管理して、ファイアウォールに対する管理情報の設定を一括しておこなえるようにして、ネットワーク管理者の労力の軽減に資するファイアウォール統括管理システムを提供することができる。

【図面の簡単な説明】

【図１】

本実施形態に係るファイアウォール統括管理システムのネットワーク構成図である。

【図２】

本実施形態に係る管理サーバ１３のハードウェア構成図である。

【図３】

本実施形態に係るファイアウォール１４ａ～１４ｄのハードウェア構成図である。

【図４】

本実施形態に係る管理端末１５のハードウェア構成図である。

【図５】

本発明に係るファイアウォール統括管理システムが、ファイアウォールの設定をする処理を模式的に示した図である。

【図６】

管理者が、設定情報を入力するときの管理端末１５上の入力画面５１を示す図である。

【図７】

管理サーバ１３上のファイアウォール構成情報テーブル２４を示す図である。

【図８】

マネージャプログラム２２が設定するファイアウォールを特定する処理を示すフローチャートである。

【図９】

経由ドメインリスト２１４の内容を状態毎に示した図である。

【図１０】

管理サーバ１３上の経由ファイアウォールテーブル２１４を示す図である。

【図１１】

管理サーバ１３上のユーザ情報テーブル２５を示す図である。

【図１２】

管理サーバ１３上のファイアウォール設定情報テーブル２１５を示す図である。

【図１３】

登録ＩＤを生成する処理を示すフローチャートである。

【図１４】

マネージャプログラム２３が各ファイアウォールに送信するリクエストパケット１５１と、エージェントプログラム３３が管理サーバ１３に送信するリプライパケット１５１１のフォーマットを示す図である。

【図１５】

管理サーバ１３上のマネージャプログラム２３と、ファイアウォール上のエージェントプログラム３３の通信プロトコルを示す図である。

【図１６】

ファイアウォール２上のユーザ登録テーブル３１２を示す図である。

【図１７】

ファイアウォール２上のアクセス制御テーブル３１３を示す図である。

【図１８】

ファイアウォール２上の経路制御テーブル３１４を示す図である。

【図１９】

管理サーバ上とファイアウォール上の両者に置かれる中継経路テーブル１７１を示す図である。

【図２０】

管理サーバ１３上のマネージャプログラム２３と、ファイアウォール上の中継

プログラム３４、およびエージェントプログラム３３の三者の通信プロトコルを示す図である。

【図２１】

ファイアウォール１上のユーザ登録テーブル３１２を示す図である。

【図２２】

ファイアウォール１上のアクセス制御テーブル３１３を示す図である。

【図２３】

ファイアウォール１上の経路制御テーブル３１４を示す図である。

【符号の説明】

１１…インターネット、１２ａ～１２ｄ…ドメイン、１３…管理サーバ、１４ａ～１４ｄ…ファイアウォール、１５…管理端末、２１…プロセッサ、２２…固定ディスク、２３…マネージャプログラム、２４…ファイアウォール構成情報テーブル、２５…ユーザ情報テーブル、２６…中継経路テーブル、２７…メモリ、２８…マネージャプログラムエリア、２９…認証・暗号通信モジュールエリア、２１０…中継経路テーブルエリア、２１１…入出力制御部、２１２…ディスプレイ・キーボード、２１３…ネットワーク制御部、２１４…経由ファイアウォールテーブルエリア、２１５…ファイアウォール設定情報テーブルエリア、３１…プロセッサ、３２…固定ディスク、３３…エージェントプログラム、３４…中継プログラム、３５…中継経路テーブル、３６…メモリ、３７…エージェントプログラムエリア、３８…中継プログラムエリア、３９…中継経路テーブルエリア、３１０…認証・暗号通信モジュールエリア、３１１…ネットワーク制御部、３１２…ユーザ登録テーブル、３１３…アクセス制御テーブル、３１４…経路制御テーブル、４１…プロセッサ、４２…固定ディスク、４３…ユーザインタフェースプログラム、４４…メモリ、４５…ユーザインタフェースプログラムエリア、４６…入出力制御部、４７…ディスプレイ・キーボード、４８…ネットワーク制御部、５１…入力画面、５２…グローバルユーザ名、５３…クライアントアドレス、５４…サーバアドレス、５５…サービス名、６１…ドメイン名フィールド、６２…ファイアウォール名フィールド、６３…隣接ドメイン名フィールド、６４ａ～６４ｆ…ドメインエントリ、７１…リスト初期化処理、７２…経由ドメイン検索

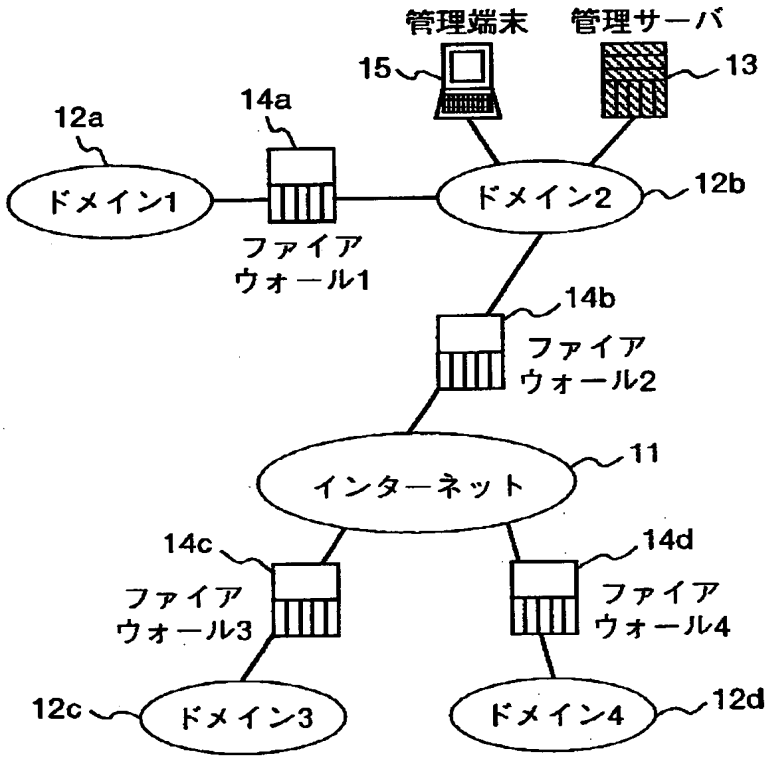
処理、７３…経由ファイアウォール取得処理、７４…隣接ドメイン名取得処理、７５…リスト要素条件分岐処理、７６…ドメイン名使用条件分岐処理、７７…経由ドメインリスト追加処理、７８…終了条件分岐処理、７９…経由ドメインリスト保存処理、７１０…経由ドメインリスト削除処理、７１１…経由ドメイン検索再帰処理、７１２…経由ドメインリスト削除処理、８１…クライアントアドレス、８２…サーバアドレス、８３…経由ファイアウォールリスト、９１…登録ＩＤフィールド、９２…認証情報フィールド、９３ａ，９３ｂ…ユーザ情報エントリ、１０１…登録ＩＤフィールド、１０２…クライアントアドレスフィールド、１０３…サーバアドレスフィールド、１０４…送信元アドレスフィールド、１０５…送信先アドレスフィールド、１０６…サービス名フィールド、１０７ａ，１０７ｂ…アクセス制御エントリ、１１１…送信先アドレスフィールド、１１２…中継先アドレスフィールド、１１３ａ，１１３ｂ…経路エントリフィールド、１２１…グローバルユーザ名フィールド、１２２…クライアントアドレスフィールド、１２３…サーバアドレスフィールド、１２４…サービス名フィールド、１２５…経由ファイアウォールリストフィールド、１２６ａ～１２６ｃ…ユーザエントリ、１３１…ユーザ登録状況確認処理、１３２…ユーザ登録条件分岐処理、１３３…登録ＩＤ生成処理、１３４…登録ＩＤ送信処理、１３５…登録ＩＤ使用状況受信処理、１３６…登録ＩＤ使用条件分岐処理、１３７…登録確定条件分岐処理、１３８…テーブル登録処理、１３９…ファイアウォール設定情報生成処理、１４１…設定対象ファイアウォールフィールド、１４２…登録ＩＤフィールド、１４３…クライアントアドレスフィールド、１４４…サーバアドレスフィールド、１４５…サービスフィールド、１４６…送信元アドレスフィールド、１４７…送信先アドレスフィールド、１４８ａ～１４８ｃ…ファイアウォール設定情報エントリ、１５１…リクエストパケット、１５２…コマンドフィールド、１５３…作業対象フィールド、１５４…登録ＩＤフィールド、１５５…クライアントアドレスフィールド、１５６…サーバアドレスフィールド、１５７…サービス名フィールド、１５８…送信元アドレスフィールド、１５９…送信先アドレスフィールド、１５１０ａ…ユーザ登録要求パケット、１５１０ｂ…アクセス制御設定要求パケット、１５１０ｃ…経路制御設定要求パケット、１５１１…リプライパケット

、１５１２…リプライコードフィールド、１５１３…コマンドフィールド、１５１４…作業対象フィールド、１５１５ａ…ユーザ登録処理結果通知パケット、１５１０ｂ…アクセス制御設定処理結果通知パケット、１５１０ｃ…経路制御設定処理結果通知パケット、１６１…接続要求処理、１６２…相互認証処理、１６３…暗号鍵取得処理、１６４…接続確認処理、１６５…リクエスト処理、１６６…設定実行処理、１６７…リプライ処理、１７１…経路制御情報テーブル、１７２…送信先アドレス、１７３…中継先アドレス、１７４ａ，１６４ｂ…経路エントリ、１８１…接続先決定処理、１８２…接続要求処理、１８３…相互認証処理、１８４…暗号鍵取得処理、１８５…接続先決定処理、１８６…接続確認処理、１８７…接続要求処理、１８８…相互認証処理、１８９…暗号鍵取得処理、１８１０…接続確認処理、１８１１…通信開始、１９１…設定対象ファイアウォール特定処理、１９２…ファイアウォール設定情報生成処理、１９３…設定情報送信処理、１９４…受信情報設定処理、１９５…接続中継処理、１９６…管理者、１９７…ユーザ、１９８…クライアント、１９９…サーバ。

【書類名】　図面

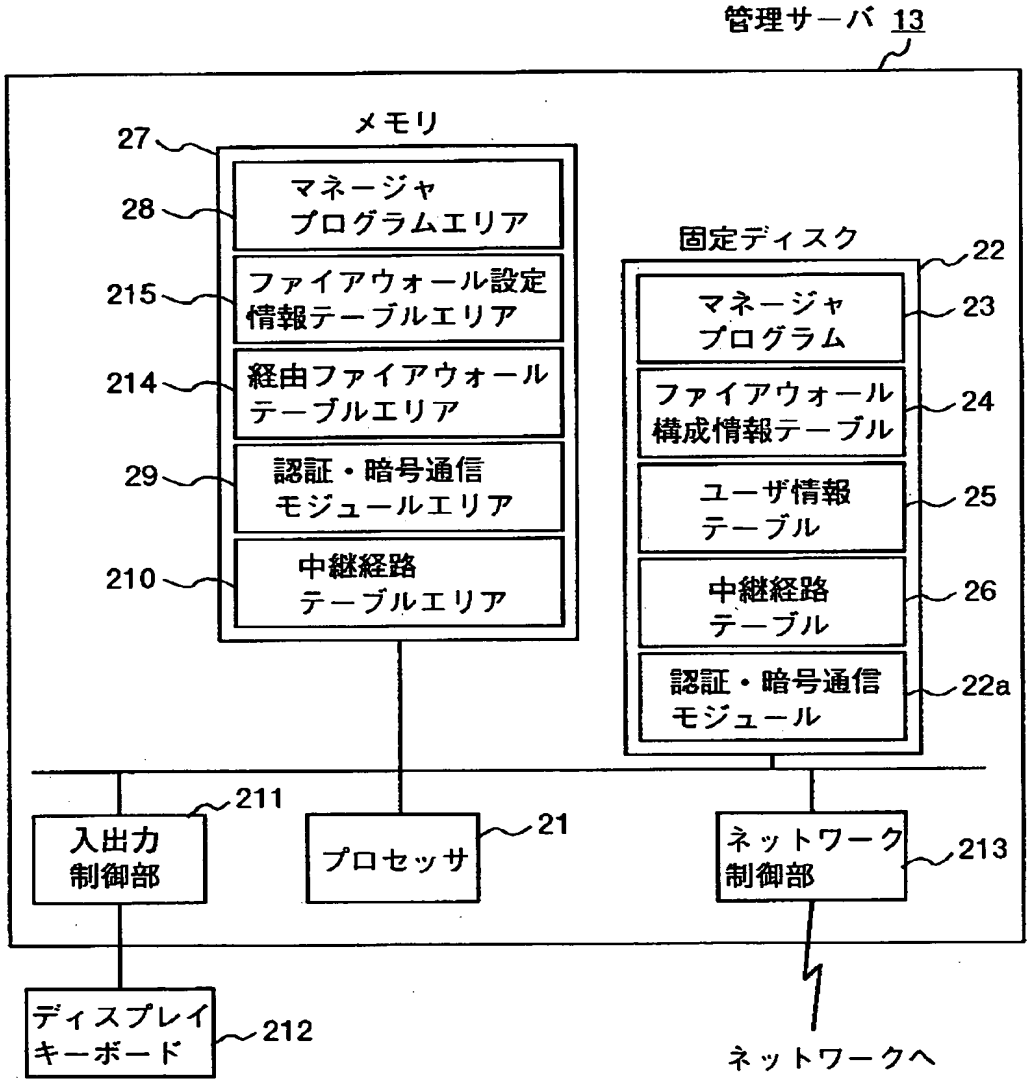
【図１】

図　1


管理端末
管理サーバ
15
13
12a
14a
ドメイン1
ファイア
ウォール1
ドメイン2
12b
14b
ファイア
ウォール2
インターネット
11
14c
14d
ファイア
ウォール3
ファイア
ウォール4
12c
ドメイン3
ドメイン4
12d

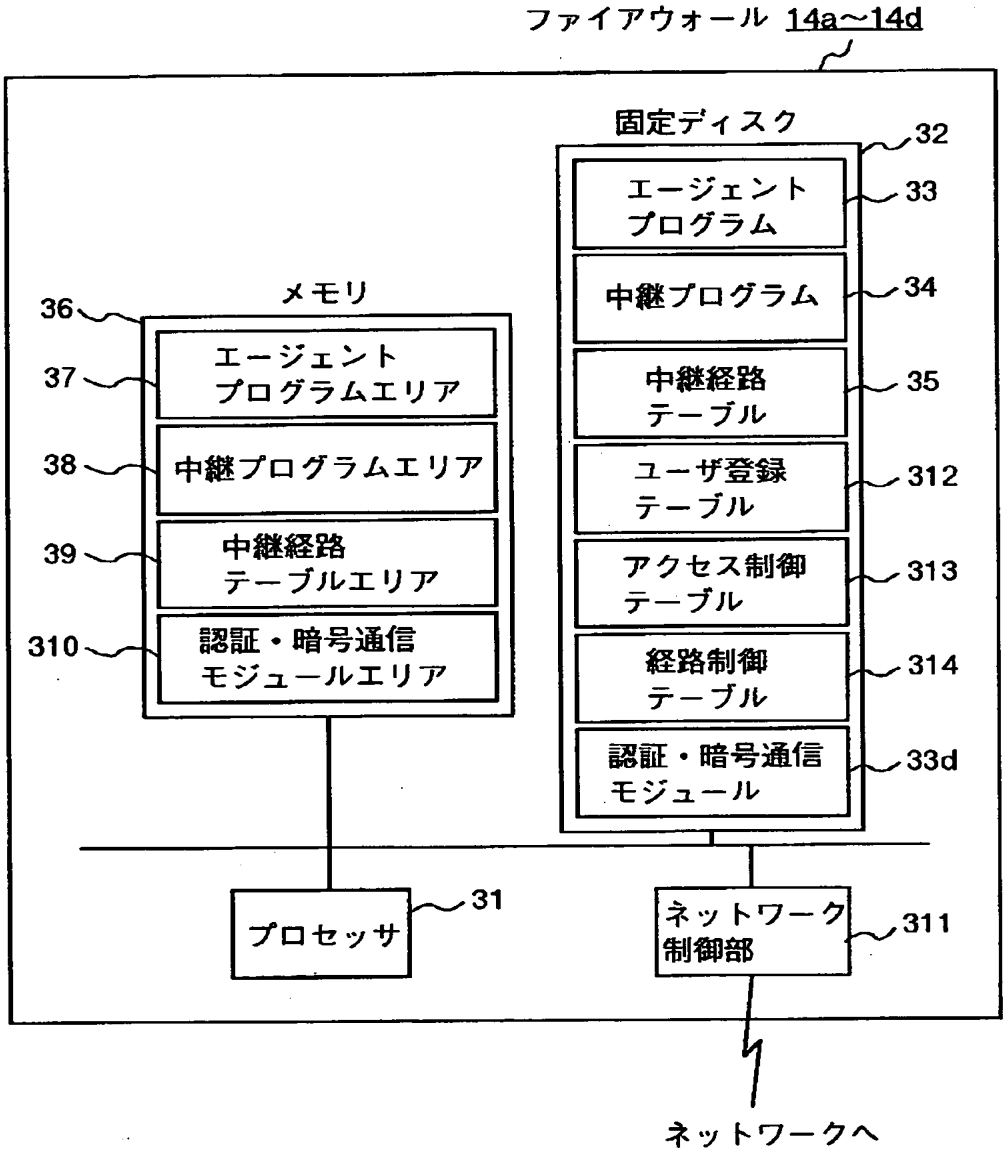
【図２】

図　２


管理サーバ 13
メモリ
27
マネージャ
プログラムエリア
28
ファイアウォール設定
情報テーブルエリア
215
経由ファイアウォール
テーブルエリア
214
認証・暗号通信
モジュールエリア
29
中継経路
テーブルエリア
210
固定ディスク
22
マネージャ
プログラム
23
ファイアウォール
構成情報テーブル
24
ユーザ情報
テーブル
25
中継経路
テーブル
26
認証・暗号通信
モジュール
22a
入出力
制御部
211
プロセッサ
21
ネットワーク
制御部
213
ディスプレイ
キーボード
212
ネットワークへ

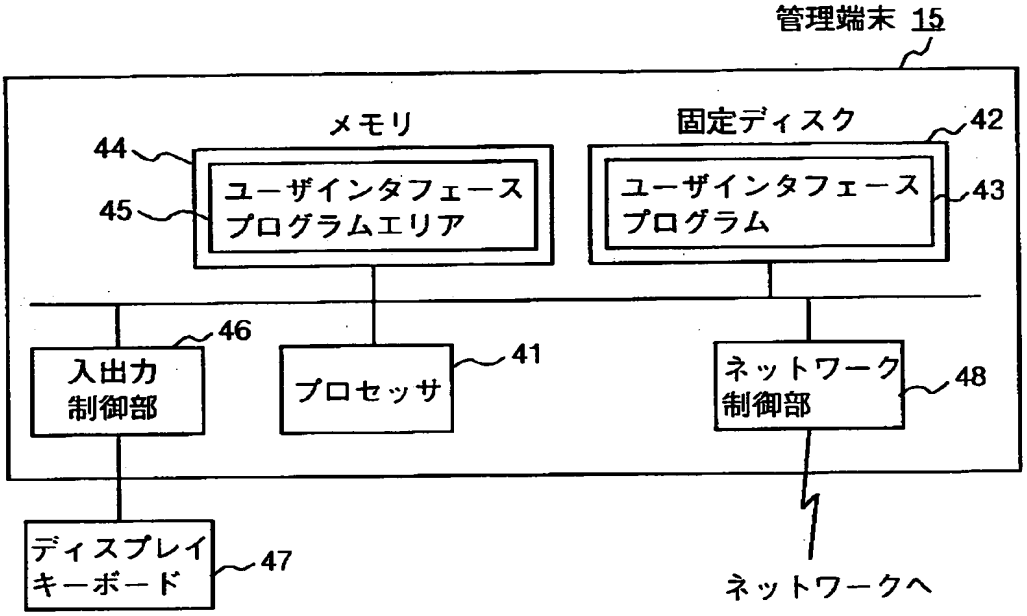
【図３】

図　3


ファイアウォール 14a～14d
固定ディスク
32
エージェント
プログラム
33
中継プログラム
34
中継経路
テーブル
35
ユーザ登録
テーブル
312
アクセス制御
テーブル
313
経路制御
テーブル
314
認証・暗号通信
モジュール
33d
メモリ
36
エージェント
プログラムエリア
37
中継プログラムエリア
38
中継経路
テーブルエリア
39
認証・暗号通信
モジュールエリア
310
プロセッサ
31
ネットワーク
制御部
311
ネットワークへ

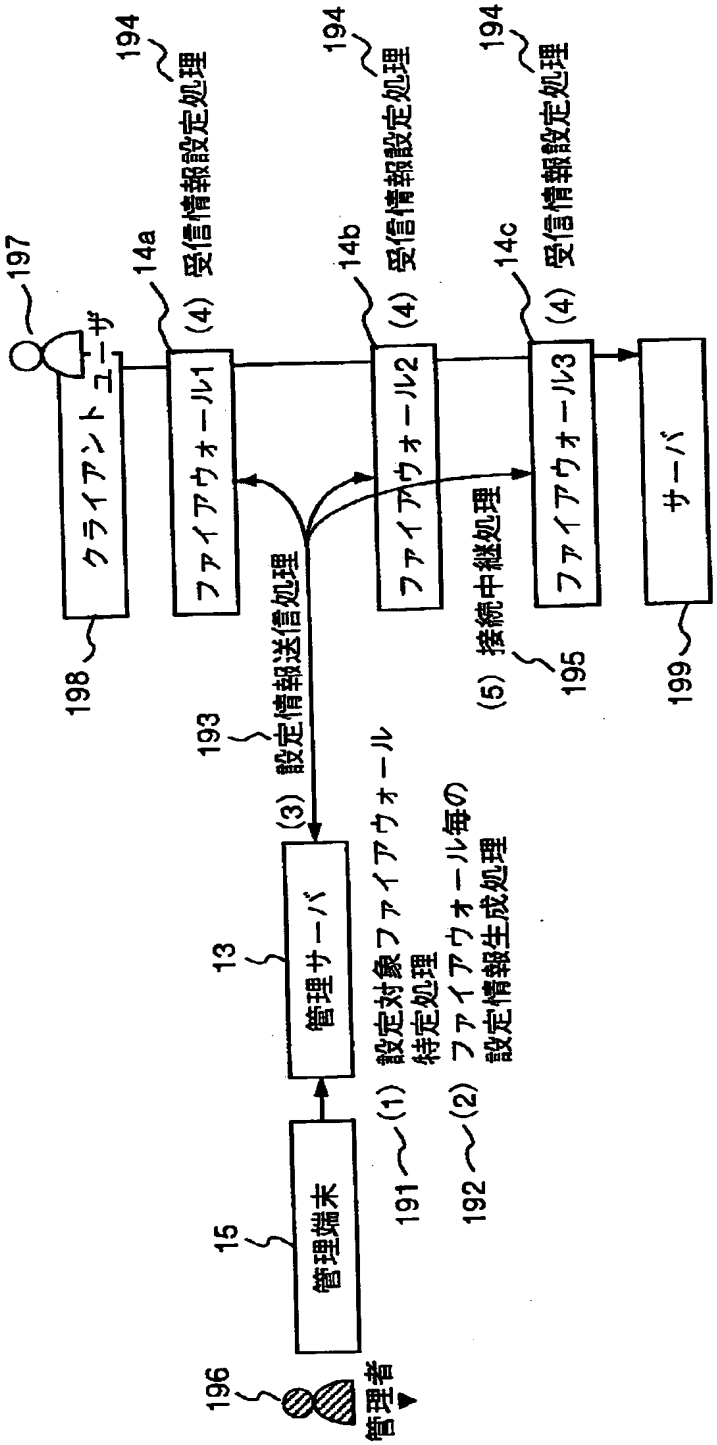
【図４】

図　4


管理端末 15
メモリ
固定ディスク
42
44
ユーザインタフェース
プログラムエリア
45
ユーザインタフェース
プログラム
43
46
入出力
制御部
プロセッサ
41
ネットワーク
制御部
48
ディスプレイ
キーボード
47
ネットワークへ

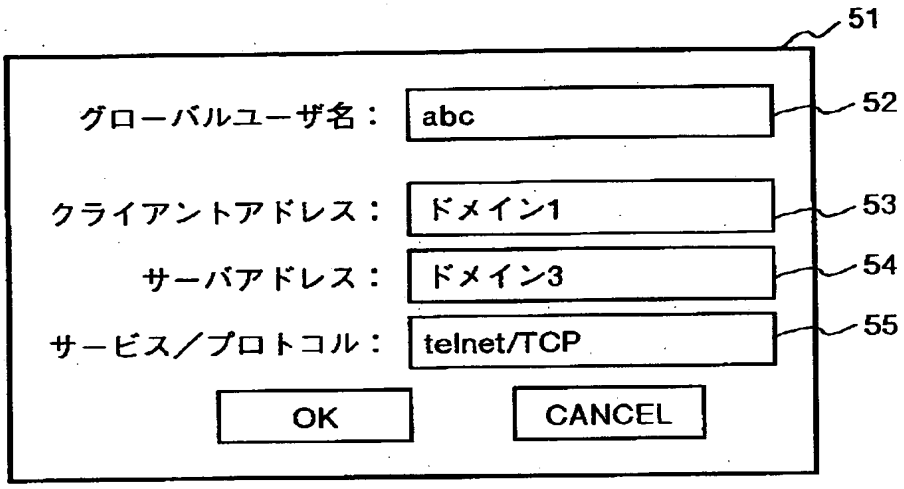
【図５】

図 5


197
ユーザ
クライアント
198
14a
194
(4) 受信情報設定処理
ファイアウォール1
14b
194
(4) 受信情報設定処理
ファイアウォール2
14c
194
(4) 受信情報設定処理
ファイアウォール3
サーバ
199
(5) 接続中継処理
195
193
(3) 設定情報送信処理
13
管理サーバ
191 (1) 設定対象ファイアウォール特定処理
192 (2) ファイアウォール毎の設定情報生成処理
15
管理端末
196
管理者

【図６】

図　6



【図７】

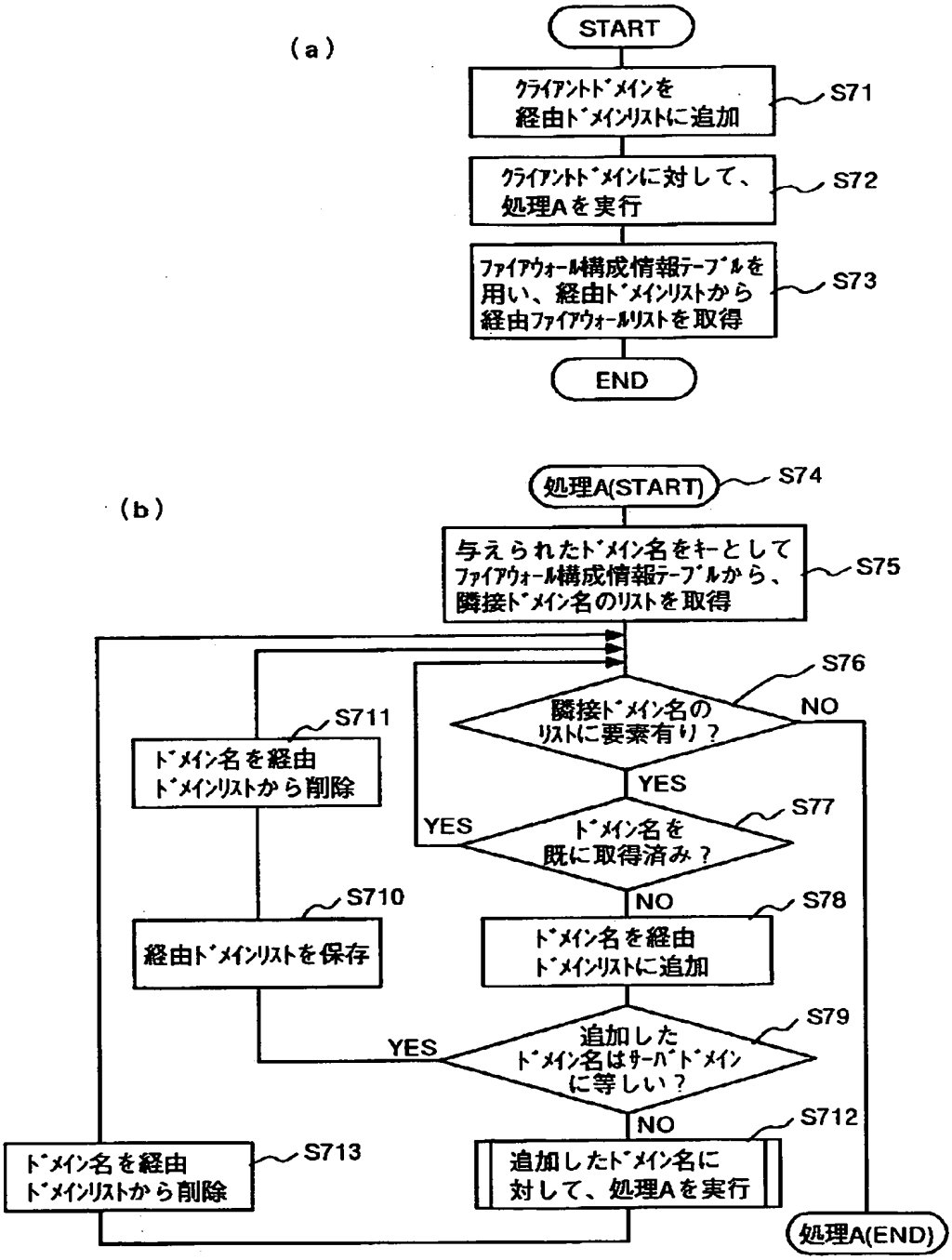
図　7

ファイアウォール構成情報テーブル 24

	61 ドメイン名	62 ファイアウォール名	63 隣接ドメイン名
64a	ドメイン1	ファイアウォール1	ドメイン2
64b	ドメイン2	ファイアウォール2	インターネット
64c	ドメイン2	ファイアウォール1	ドメイン1
64d	ドメイン3	ファイアウォール3	インターネット
64e	ドメイン4	ファイアウォール4	インターネット
64f	インターネット	ファイアウォール2	ドメイン2
64g	インターネット	ファイアウォール3	ドメイン3
64h	インターネット	ファイアウォール4	ドメイン4

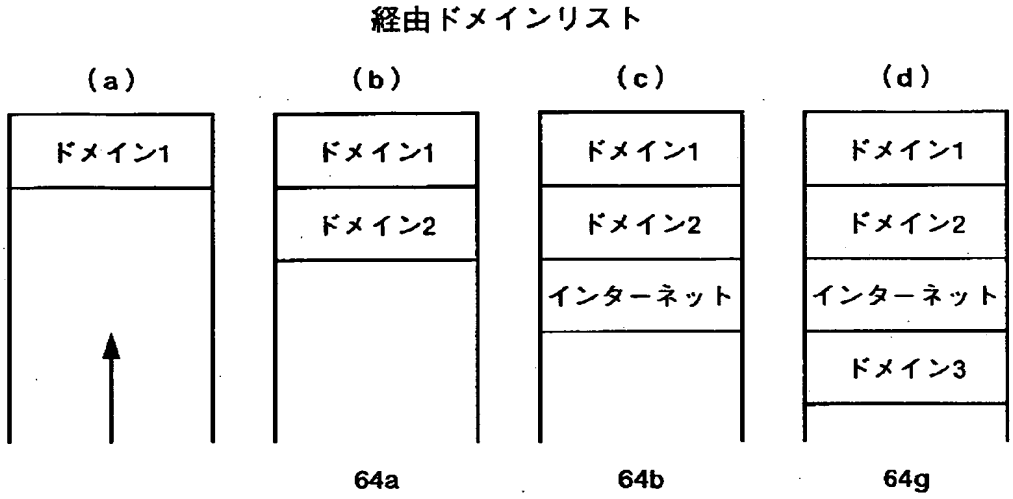
【図８】

図　8


(a)
START
ｸﾗｲｱﾝﾄﾄﾞﾒｲﾝを
経由ﾄﾞﾒｲﾝﾘｽﾄに追加
S71
ｸﾗｲｱﾝﾄﾄﾞﾒｲﾝに対して、
処理Aを実行
S72
ﾌｧｲｱｳｫｰﾙ構成情報ﾃｰﾌﾞﾙを
用い、経由ﾄﾞﾒｲﾝﾘｽﾄから
経由ﾌｧｲｱｳｫｰﾙﾘｽﾄを取得
S73
END
(b)
処理A(START)
S74
与えられたﾄﾞﾒｲﾝ名をｷｰとして
ﾌｧｲｱｳｫｰﾙ構成情報ﾃｰﾌﾞﾙから、
隣接ﾄﾞﾒｲﾝ名のﾘｽﾄを取得
S75
S76
隣接ﾄﾞﾒｲﾝ名の
ﾘｽﾄに要素有り？
NO
YES
S77
YES
ﾄﾞﾒｲﾝ名を
既に取得済み？
S711
ﾄﾞﾒｲﾝ名を経由
ﾄﾞﾒｲﾝﾘｽﾄから削除
NO
S78
ﾄﾞﾒｲﾝ名を経由
ﾄﾞﾒｲﾝﾘｽﾄに追加
S710
経由ﾄﾞﾒｲﾝﾘｽﾄを保存
S79
追加した
ﾄﾞﾒｲﾝ名はｻｰﾊﾞﾄﾞﾒｲﾝ
に等しい？
YES
NO
S712
追加したﾄﾞﾒｲﾝ名に
対して、処理Aを実行
S713
ﾄﾞﾒｲﾝ名を経由
ﾄﾞﾒｲﾝﾘｽﾄから削除
処理A(END)

【図９】

図　９


経由ドメインリスト
(a)
(b)
(c)
(d)
ドメイン1
ドメイン1
ドメイン2
ドメイン1
ドメイン2
インターネット
ドメイン1
ドメイン2
インターネット
ドメイン3
64a
64b
64g

【図１０】

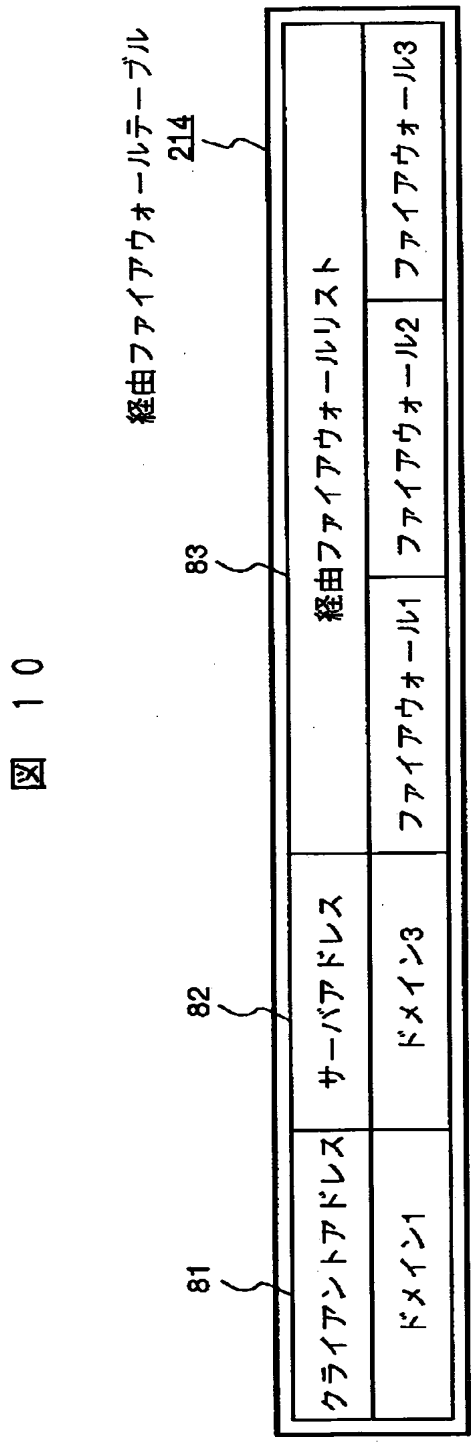
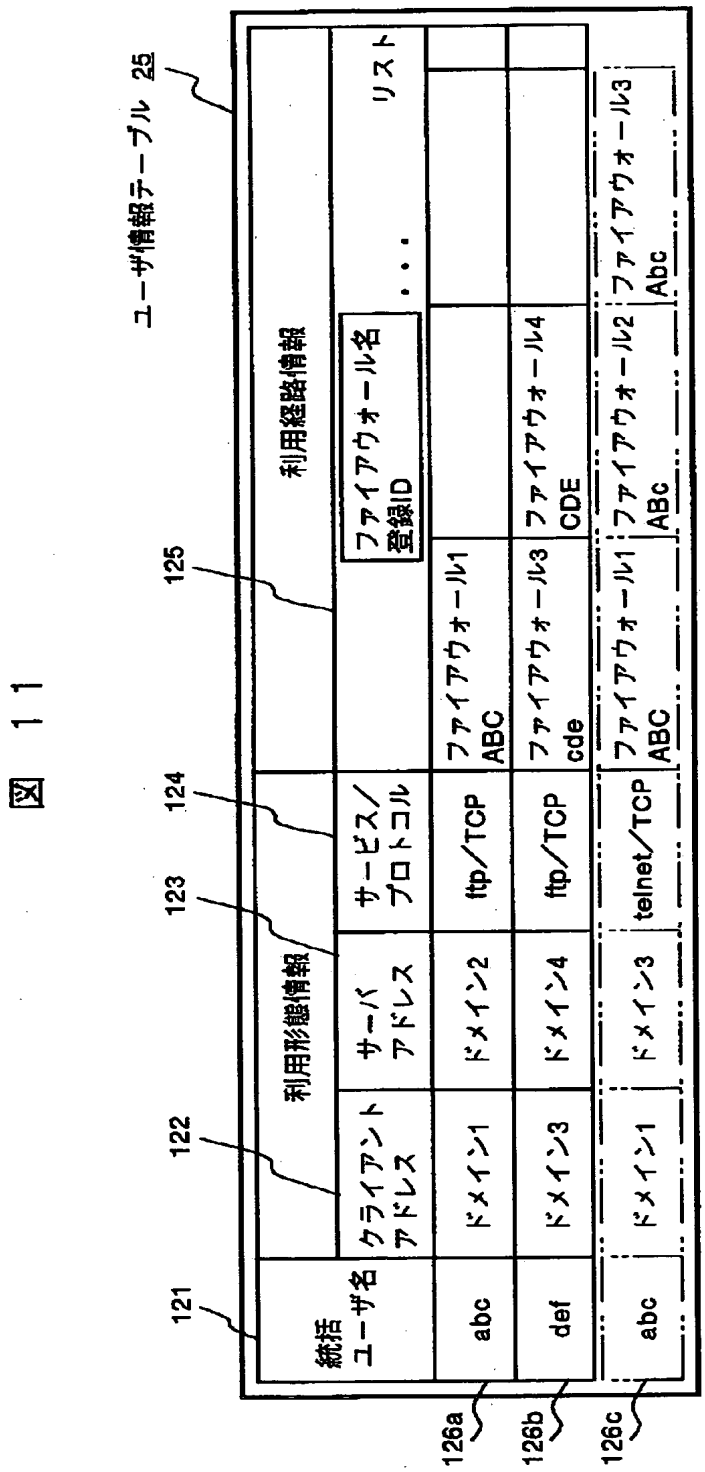

経由ファイアウォールテーブル
214
83
82
81
クライアントアドレス
サーバアドレス
経由ファイアウォールリスト
ドメイン1
ドメイン3
ファイアウォール1
ファイアウォール2
ファイアウォール3

図　１０

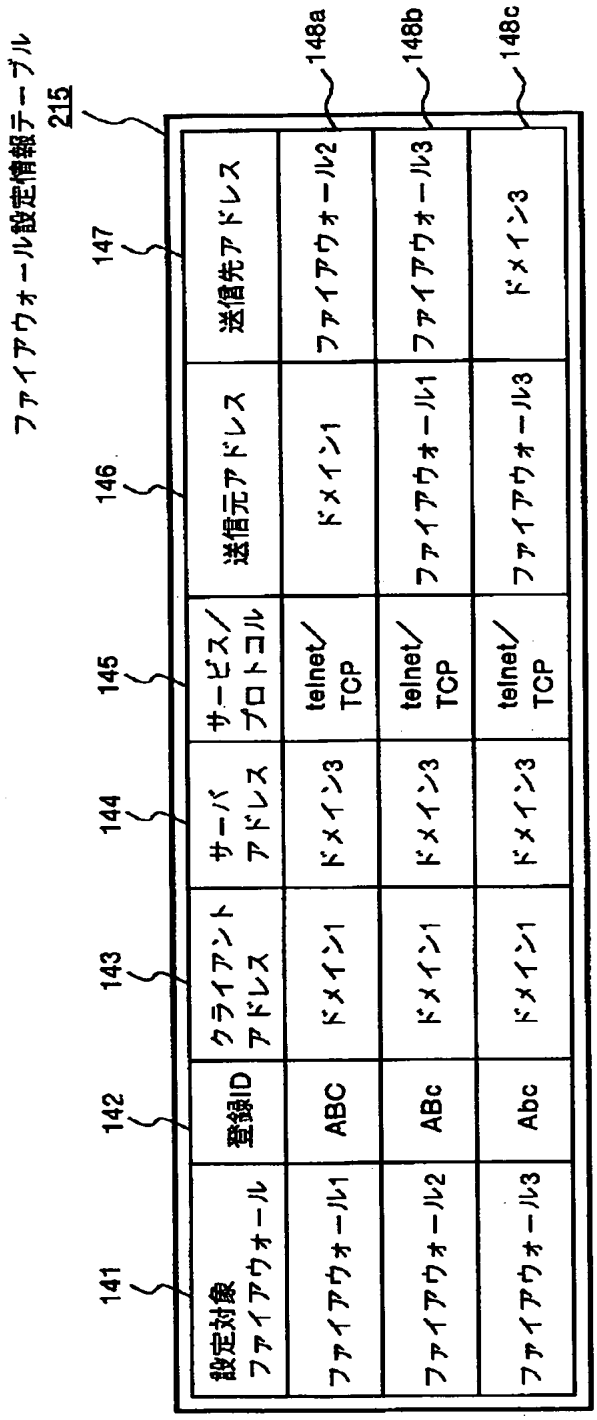
【図１１】

図　１１


ユーザ情報テーブル 25
121
122
123
124
125
統括ユーザ名
利用形態情報
クライアントアドレス
サーバアドレス
サービス／プロトコル
利用経路情報
ファイアウォール名登録ID
リスト
abc
ドメイン1
ドメイン2
ftp／TCP
ファイアウォール1 ABC
def
ドメイン3
ドメイン4
ftp／TCP
ファイアウォール3 cde
ファイアウォール4 CDE
abc
ドメイン1
ドメイン3
telnet／TCP
ファイアウォール1 ABC
ファイアウォール2 ABc
ファイアウォール3 Abc
126a
126b
126c

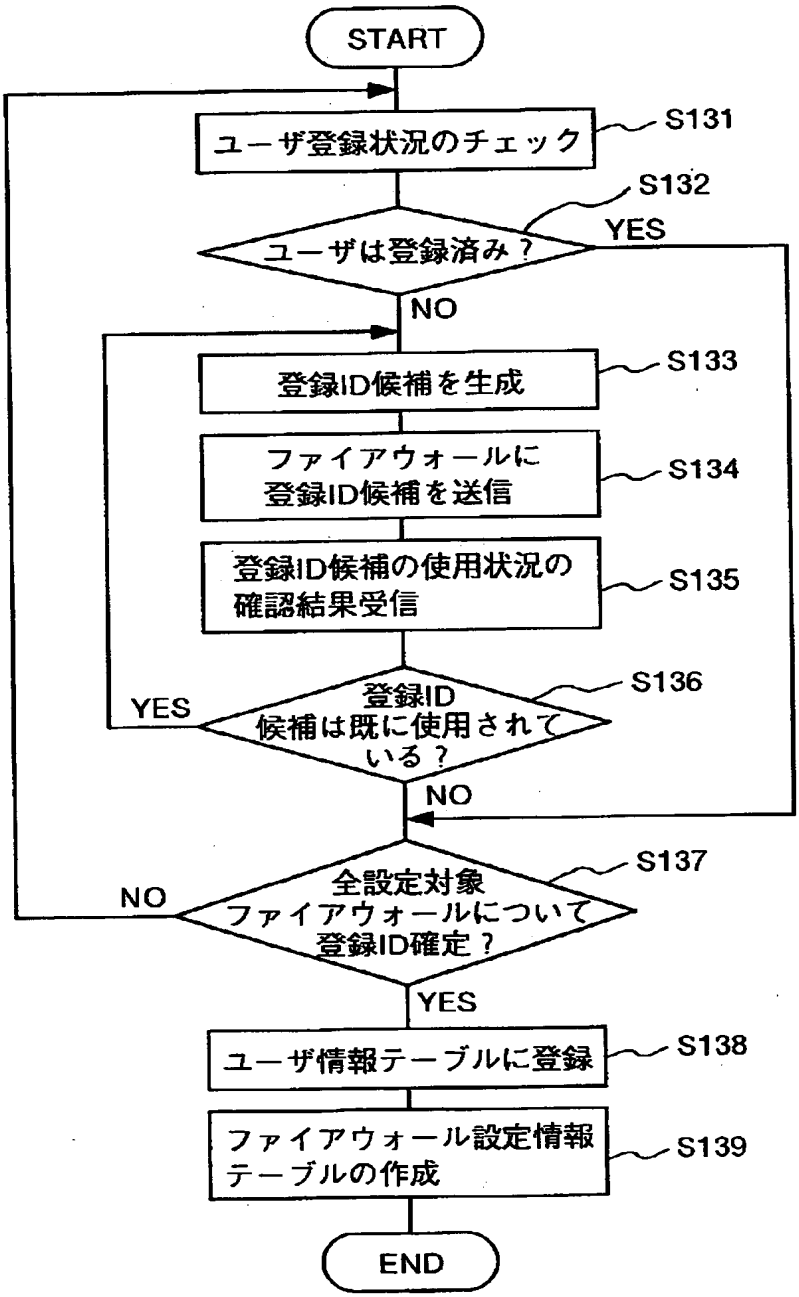
【図１２】

図　１２


ファイアウォール設定情報テーブル
215
141
142
143
144
145
146
147
148a
148b
148c
設定対象ファイアウォール
登録ID
クライアントアドレス
サーバアドレス
サービス/プロトコル
送信元アドレス
送信先アドレス
ファイアウォール1
ABC
ドメイン1
ドメイン3
telnet/TCP
ドメイン1
ファイアウォール2
ファイアウォール2
ABc
ドメイン1
ドメイン3
telnet/TCP
ドメイン1
ファイアウォール3
ファイアウォール3
Abc
ドメイン1
ドメイン3
telnet/TCP
ファイアウォール3
ドメイン3

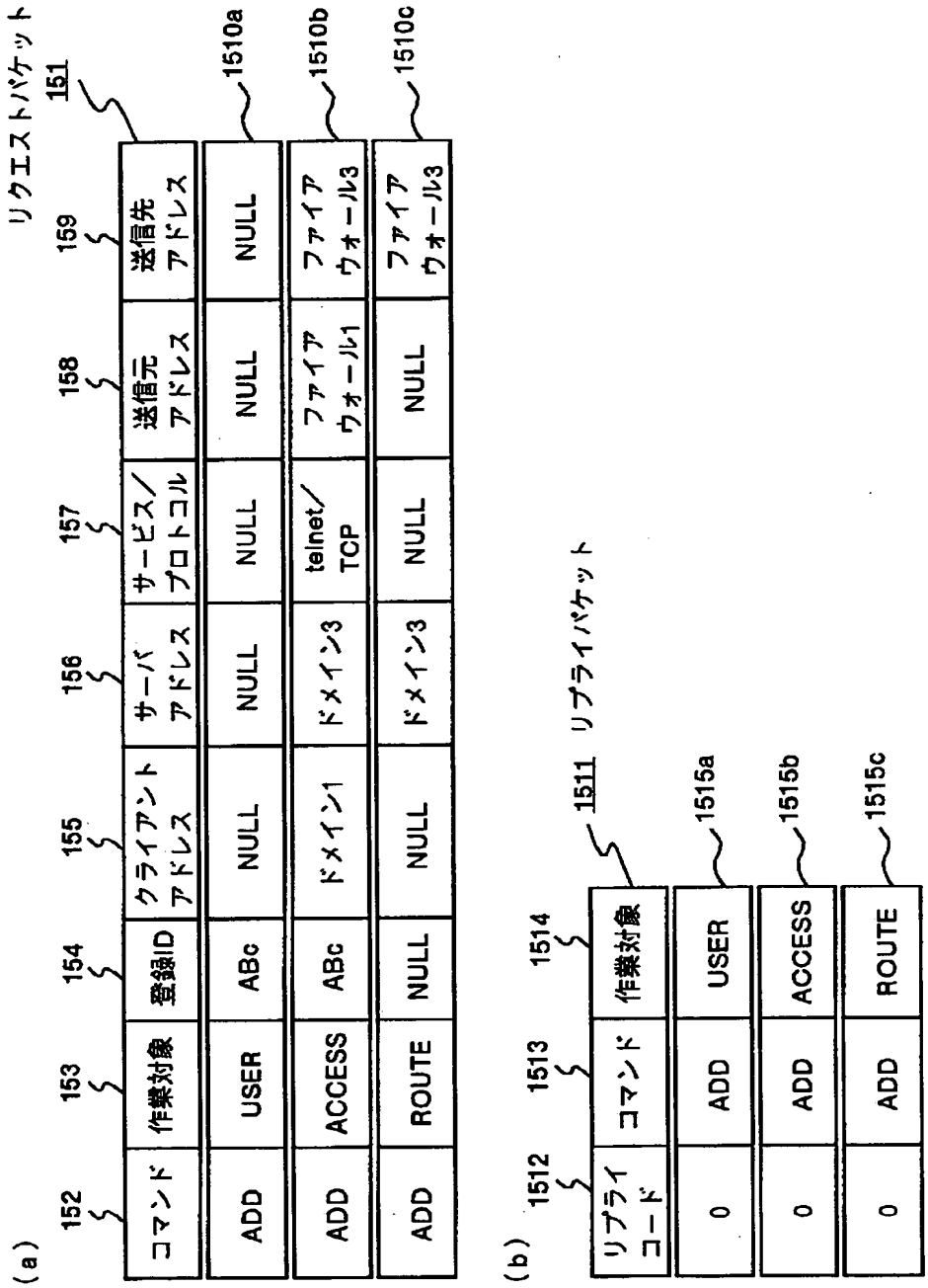
【図１３】

図　１３


START
ユーザ登録状況のチェック
S131
S132
ユーザは登録済み？
YES
NO
登録ID候補を生成
S133
ファイアウォールに
登録ID候補を送信
S134
登録ID候補の使用状況の
確認結果受信
S135
登録ID
候補は既に使用されて
いる？
S136
YES
NO
全設定対象
ファイアウォールについて
登録ID確定？
S137
NO
YES
ユーザ情報テーブルに登録
S138
ファイアウォール設定情報
テーブルの作成
S139
END

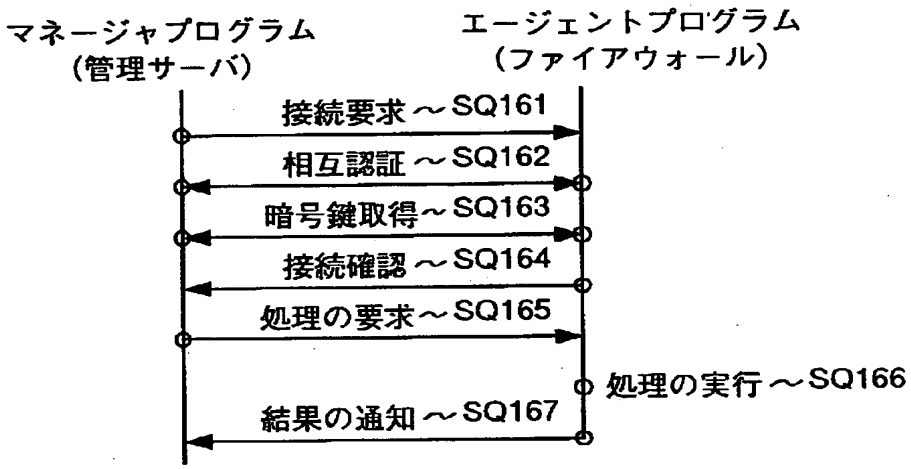
【図１４】

図　１４


(a)
リクエストパケット
151
152
コマンド
153
作業対象
154
登録ID
155
クライアントアドレス
156
サーバアドレス
157
サービス／プロトコル
158
送信元アドレス
159
送信先アドレス
1510a
ADD
USER
ABc
NULL
NULL
NULL
NULL
NULL
1510b
ADD
ACCESS
ABc
ドメイン1
ドメイン3
telnet／TCP
ファイアウォール1
ファイアウォール3
1510c
ADD
ROUTE
NULL
NULL
ドメイン3
NULL
NULL
ファイアウォール3
(b)
リプライパケット
1511
1512
リプライコード
1513
コマンド
1514
作業対象
1515a
0
ADD
USER
1515b
0
ADD
ACCESS
1515c
0
ADD
ROUTE

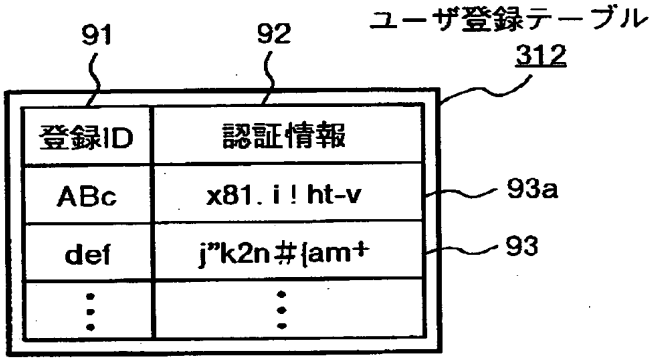
【図１５】

図　１５



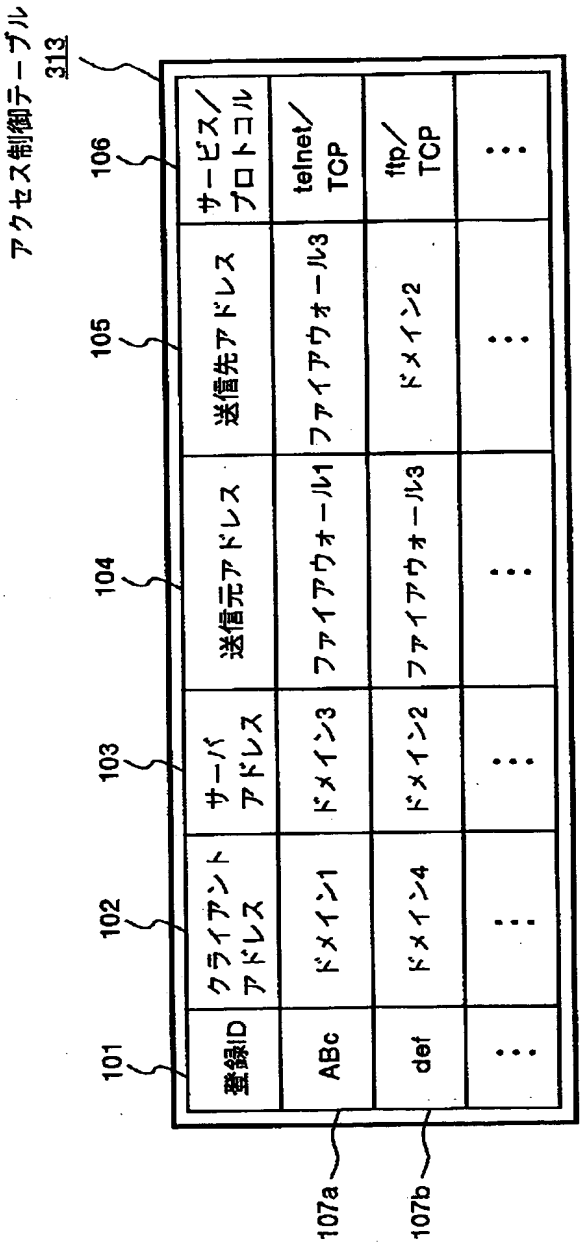
【図１６】

図　１６



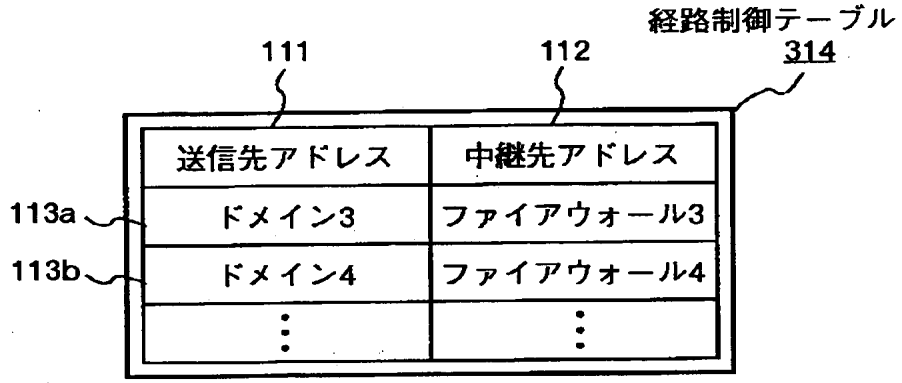
【図１７】

図１７


アクセス制御テーブル
313
101
102
103
104
105
106
登録ID
クライアントアドレス
サーバアドレス
送信元アドレス
送信先アドレス
サービス／プロトコル
ABc
ドメイン1
ドメイン3
ファイアウォール1
ファイアウォール3
telnet／TCP
def
ドメイン4
ドメイン2
ファイアウォール3
ドメイン2
ftp／TCP
107a
107b

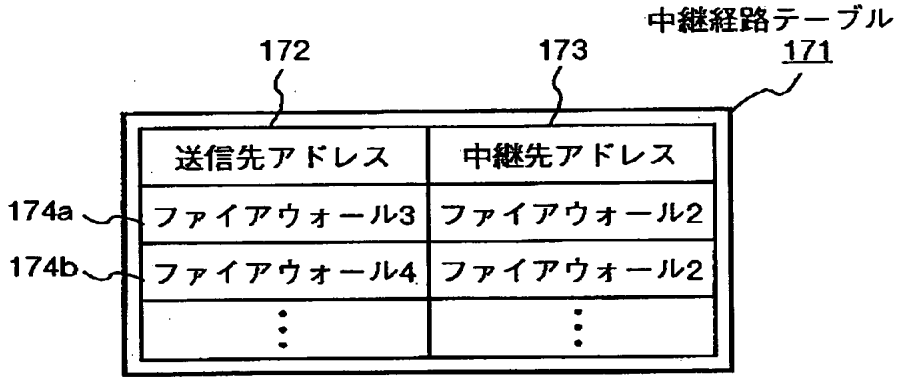
【図１８】

図　１８



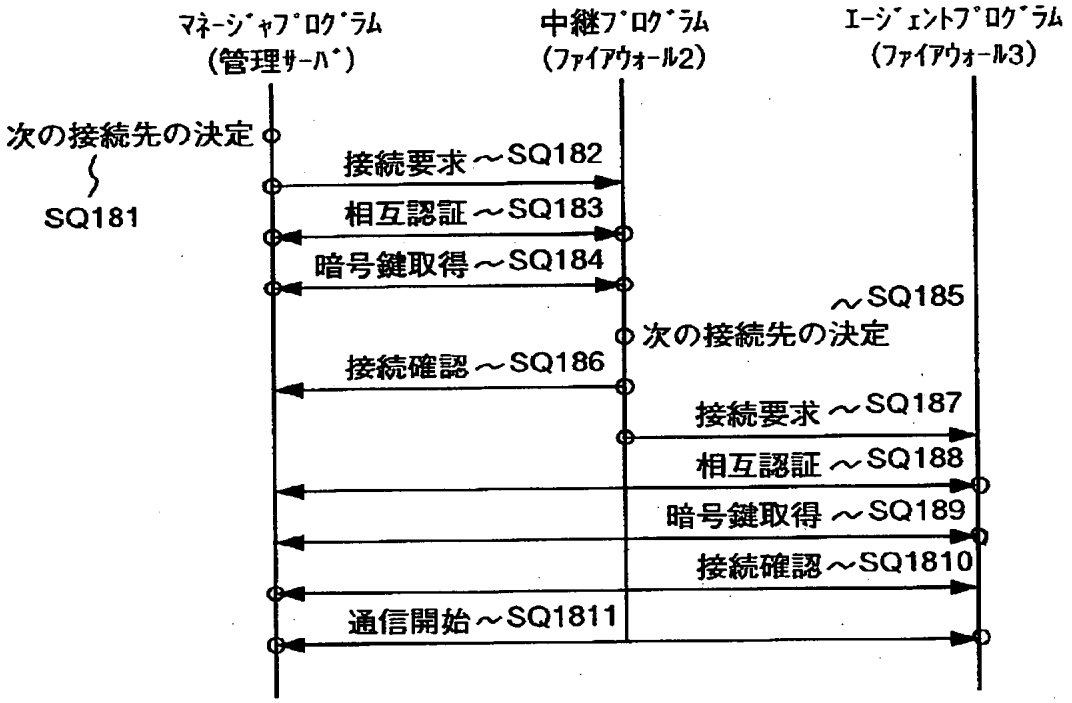
【図１９】

図　１９



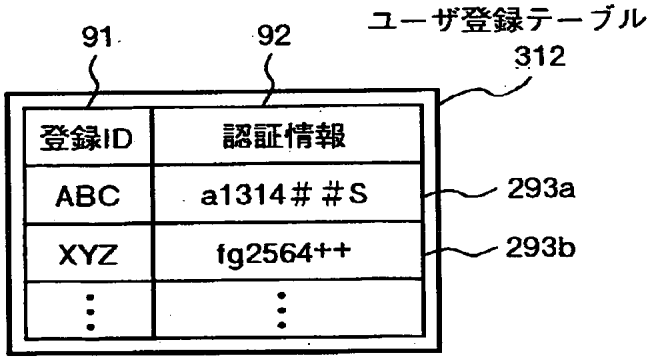
【図２０】

図　２０



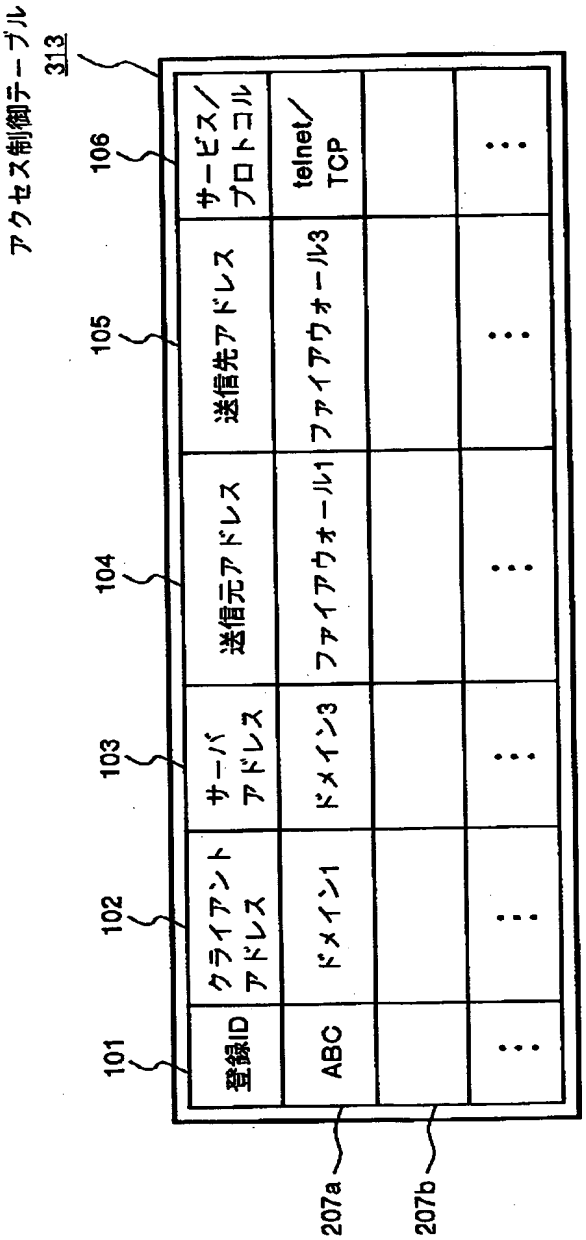
【図２１】

図　２１



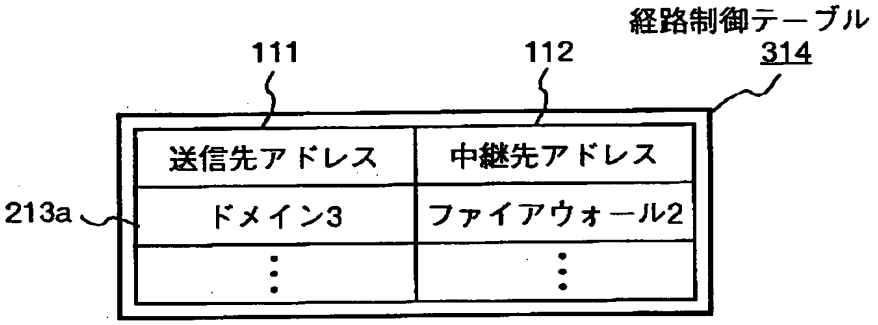
【図２２】

図　２２


アクセス制御テーブル
313
101
102
103
104
105
106
登録ID
クライアントアドレス
サーバアドレス
送信元アドレス
送信先アドレス
サービス／プロトコル
ABC
ドメイン1
ドメイン3
ファイアウォール1
ファイアウォール3
telnet／TCP
207a
207b

【図２３】

図　２３



【書類名】　　要約書

【要約】

【課題】イントラネット、ＶＰＮのような複数のファイアウォールを有するネットワークシステムにおいて、ファイアウォールに対する管理情報の設定を一括しておこなえるようにして、ネットワーク管理者の労力の軽減に資するようにする。

【解決手段】ネットワークの管理単位間にファイアウォールを設け、ファイアウォールに管理情報の設定をおこなうための管理サーバを置いて、その管理サーバのマネージャプログラムから、設定情報を送信することによって、あるファイアウォールに隔てられて直接通信できないファイアウォールに対しても、管理情報の設定をおこなう。また、途中のファイアウォールは、接続の中継をする。

【選択図】　　図５

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005108
【住所又は居所】　東京都千代田区神田駿河台四丁目６番地
【氏名又は名称】　株式会社日立製作所
【代理人】　申請人
【識別番号】　100061893
【住所又は居所】　東京都中央区日本橋茅場町二丁目九番八号　友泉茅場町ビル　日東国際特許事務所
【氏名又は名称】　高橋　明夫
【選任した代理人】
【識別番号】　100086656
【住所又は居所】　東京都中央区日本橋茅場町二丁目九番八号　友泉茅場町ビル　日東国際特許事務所
【氏名又は名称】　田中　恭助

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所